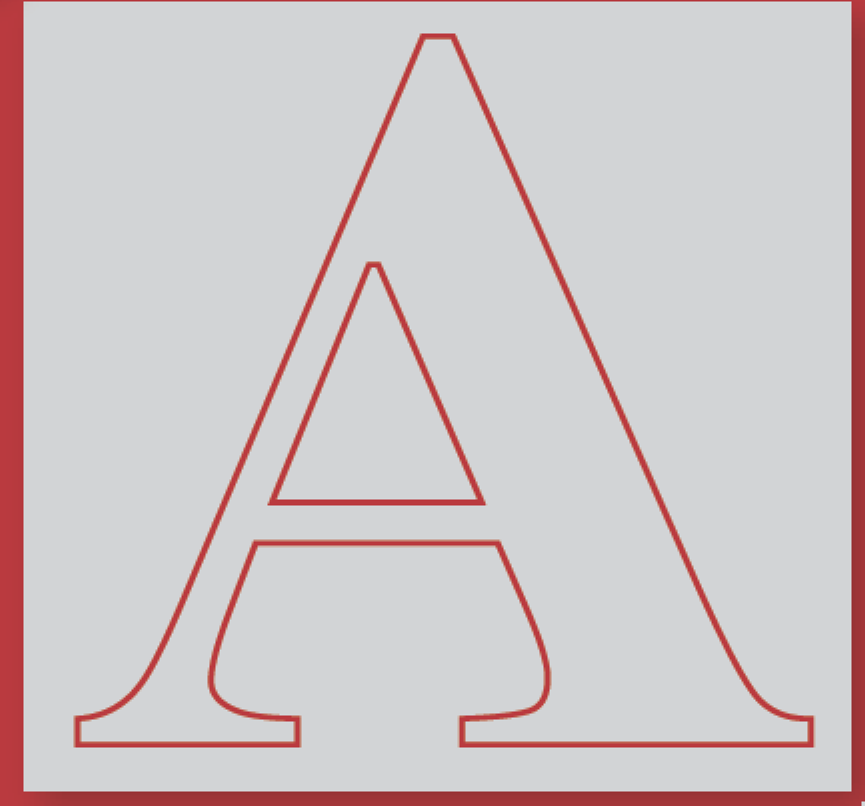
21世纪高等学校计算机专业实用规划教材

计算机网络安全技术

王 群 编著







清华大学出版社

21世纪高等学校计算机专业实用规划教材

计算机网络安全技术

王　群　编著

清华大学出版社
北　京

内 容 简 介

本书是一本面向普通高等院校本科教学要求的教材，是理论与实践有机结合的研究成果，也是作者长期从事计算机网络教学、网络安全设计、网络管理与维护的经验总结。为了使内容安排符合教学要求，并尽可能地贴近实际应用，解决实际问题，本书在内容选择上既注重基本理论和概念的讲述，又紧紧抓住目前网络安全领域的关键技术和用户普遍关注的热点问题，对内容进行了合理规划。

本书共分 9 章，主要内容包括计算机网络安全概述、数据加密技术及应用、PKI/PMI 技术及应用、身份认证技术、TCP/IP 体系的协议安全、计算机病毒、木马和间谍软件与防治、网络攻击与防范、防火墙技术及应用、VPN 技术及应用等。

本书主要针对普通高等院校计算机及相关专业本科层次的教学要求而编写，其中大量的实训内容可供高职高专和有关培训机构使用，本书也可供从事网络安全设计和管理的技术人员阅读、参考。

图书在版编目（CIP）数据

计算机网络安全技术/王群编著. —北京：清华大学出版社，2008.8
（21 世纪高等学校计算机专业实用规划教材）
ISBN 978-7-302-17778-4

Ⅰ. 计…　Ⅱ. 王…　Ⅲ. 计算机网络—安全技术—高等学校—教材　Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字(2008)第 078420 号

责任编辑：魏江江　薛　阳
责任校对：焦丽丽
责任印制：

出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**邮　　编**：100084
社　总　机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质　量　反　馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：
装 订 者：
经　　销：全国新华书店
开　　本：185×260　**印　张**：19.25　　**字　　数**：469 千字
版　　次：2008 年 8 月第 1 版　　**印　　次**：2008 年 8 月第1 次印刷
印　　数：1～　000
定　　价：　.00 元

本书如存在文字不清、漏印、缺页、倒页、脱页等印装质量问题，请与清华大学出版社出版部联系调换。
联系电话：010-62770177 转 3103　　产品编号：

出版说明

随着我国改革开放的进一步深化，高等教育也得到了快速发展，各地高校紧密结合地方经济建设发展需要，科学运用市场调节机制，加大了使用信息科学等现代科学技术提升、改造传统学科专业的投入力度，通过教育改革合理调整和配置了教育资源，优化了传统学科专业，积极为地方经济建设输送人才，为我国经济社会的快速、健康和可持续发展以及高等教育自身的改革发展做出了巨大贡献。但是，高等教育质量还需要进一步提高以适应经济社会发展的需要，不少高校的专业设置和结构不尽合理，教师队伍整体素质亟待提高，人才培养模式、教学内容和方法需要进一步转变，学生的实践能力和创新精神亟待加强。

教育部一直十分重视高等教育质量工作。2007 年 1 月，教育部下发了《关于实施高等学校本科教学质量与教学改革工程的意见》，计划实施“高等学校本科教学质量与教学改革工程（简称‘质量工程’）”，通过专业结构调整、课程教材建设、实践教学改革、教学团队建设等多项内容，进一步深化高等学校教学改革，提高人才培养的能力和水平，更好地满足经济社会发展对高素质人才的需要。在贯彻和落实教育部“质量工程”的过程中，各地高校发挥师资力量强、办学经验丰富、教学资源充裕等优势，对其特色专业及特色课程（群）加以规划、整理和总结，更新教学内容、改革课程体系，建设了一大批内容新、体系新、方法新、手段新的特色课程。在此基础上，经教育部相关教学指导委员会专家的指导和建议，清华大学出版社在多个领域精选各高校的特色课程，分别规划出版系列教材，以配合“质量工程”的实施，满足各高校教学质量和教学改革的需要。

本系列教材立足于计算机专业课程领域，以专业基础课为主、专业课为辅，横向满足高校多层次教学的需要。在规划过程中体现了如下一些基本原则和特点。

（1）反映计算机学科的最新发展，总结近年来计算机专业教学的最新成果。内容先进，充分吸收国外先进成果和理念。

（2）反映教学需要，促进教学发展。教材要适应多样化的教学需要，正确把握教学内容和课程体系的改革方向，融合先进的教学思想、方法和手段，体现科学性、先进性和系统性，强调对学生实践能力的培养，为学生知识、能力、素质协调发展创造条件。

（3）实施精品战略，突出重点，保证质量。规划教材把重点放在公共基础课和专业基础课的教材建设上；特别注意选择并安排一部分原来基础比较好的优秀教材或讲义修订再版，逐步形成精品教材；提倡并鼓励编写体现教学质量和教学改革成果的教材。

（4）主张一纲多本，合理配套。专业基础课和专业课教材配套，同一门课程可以有针对不同层次、面向不同应用的多本具有各自内容特点的教材。处理好教材统一性与多样化，基本教材与辅助教材、教学参考书，文字教材与软件教材的关系，实现教材系列资源配套。

（5）依靠专家，择优选用。在制定教材规划时依靠各课程专家在调查研究本课程教材

建设现状的基础上提出规划选题。在落实主编人选时，要引入竞争机制，通过申报、评审确定主编。书稿完成后要认真实行审稿程序，确保出书质量。

繁荣教材出版事业，提高教材质量的关键是教师。建立一支高水平教材编写梯队才能保证教材的编写质量和建设力度，希望有志于教材建设的教师能够加入到我们的编写队伍中来。

21世纪高等学校计算机专业实用规划教材

联系人：魏江江 weijj@tup.tsinghua.edu.cn

前　言

如今，计算机网络的应用已延伸到全球的各个角落和领域，正在对人们的工作、生活产生前所未有的影响，如同电力、交通一样日益成为人们生活中不可缺少的组成部分。与此同时，随着网络规模的不断扩大，以及人们对网络知识的了解越来越深入，网络中的攻击等不安全因素越来越多，已经严重威胁到网络与信息的安全。计算机网络的安全已经成为一个备受全球关注的问题。

计算机网络与信息安全技术的核心问题是对计算机和网络系统进行有效的防护。网络安全防护涉及的面非常广，从技术层面上分，主要包括数据加密、身份认证、入侵检测、入侵保护、病毒防护和虚拟专用网等方面，这些技术中有些是主动防御，有些是被动保护，有些则是为安全研究提供支撑和平台。本书在写作过程中强调了以下几点。

一是尽可能用通俗易懂的语言来描述晦涩的理论阐述。在计算机网络安全这门课程中涉及到了大量的概念、理论体系、算法和协议，如何用通俗易懂的语言来描述这些抽象的专业术语是本书的一个侧重点。为此，在写作过程中作者尽可能用简捷明快的语言来阐述理论，而不是照搬文献和标准文档。

二是通过大量直观的图例来描述复杂的工作原理和操作流程。在一些国家的计算机专业教育中，有图解(diagram)或映像(map)这门课，旨在通过易于理解的图例来直观地描述网络的结构、工作流程及实现原理。本书在写作过程中采用了大量的图例和表格来描述复杂的网络安全实现原理。

三是理论与实践的有机结合。理论与实践之间的脱节是目前许多计算机专业教材普遍存在的问题，有些教材过于强调理论阐述而忽视实践操作，而有些图书则只注重讲述操作步骤而忽视了理论讲解。本书一方面强调对基本概念、理论、算法和协议的讲解，同时尽可能地通过实际操作来验证相关的理论。

四是内容新颖翔实。计算机网络技术的发展非常迅速，为了使学生在走出校门后能够将所学知识应用到具体工作中，在教材内容的选择上必须考虑到与实际应用之间的有机结合。本书在写作过程中参阅了大量的研究成果和文献资料，以求内容新颖，讲解翔实。

五是注重内容讲解时的完整性。网络安全涉及的面较广，许多应用的实现需要大量理论的支持。本书在写作过程中充分考虑到内容完整性，对所涉及到的但在本书中没有单独讲述的内容进行了实时介绍或给出了文献出处，以便读者查阅。

本书共分为9章，主要内容包括计算机网络安全概述、数据加密技术及应用、PKI/PMI技术及应用、身份认证技术、TCP/IP体系的协议安全、计算机病毒、木马和间谍软件与防治、网络攻击与防范、防火墙技术及应用和VPN技术及应用等内容。

在本书的编写过程中，作者参考了大量的国内外文献资料，其中部分文献的出处并未全

部列出。对涉及到的每一个实验操作都在实验室或真实网络环境中进行了测试，以保证实验操作步骤和内容的正确性。其中，部分实验和应用来自作者单位真实的网络环境。

在本书编写过程中，得到了清华大学出版社的大力支持，也得到了作者家人及很多同事的帮助，其中李馥娟、郭亚峰、刘庆航、宋玲华、张卫东、聂明辉和陶慎亮等老师负责了部分实验的测试和文字的校对工作，借此机会向他们表示衷心的感谢。由于作者研究水平有限，书中难免还存在一些缺点和错误，殷切希望广大教师、科研人员和读者批评指正。

计算机网络安全与计算机网络管理属于同一范畴的两个研究和应用分支，两者之间的联系非常紧密，而且都在快速地发展。为此，作者同时编写了《计算机网络管理技术》一书，并由清华大学出版社出版。

目　录

第 1 章　计算机网络安全概述

今天,IP 网络几乎成为现代计算机网络的代名词。IP 网络存在的设计缺陷和安全隐患也逐渐暴露出来。随着计算机网络应用范围的不断扩展,大量基于 IP 网络的应用层出不穷,这更加剧了网络的负担,安全问题越加突出。本章以 IP 网络为主,将从网络安全概念、安全现状、安全策略和热点技术等方面,对计算机网络的安全进行综述性介绍。

1.1　计算机网络安全研究的动因

现在广泛使用的基于 IPv4 通信协议的网络,在设计之初就存在着大量缺陷和安全隐患。虽然下一个版本 IPv6 在一定程度上将解决 IPv4 中存在的安全问题,但是 IPv6 走向全面应用还需要较长的时间。同时,从 IPv4 网络的应用历史来看,许多安全问题也是随着应用的出现而暴露出来的,所以不能肯定地讲 IPv6 网络的应用就一定能够解决 IPv4 中存在的所有安全问题。

1.1.1　网络自身的设计缺陷

如果对比分析 PSTN、ATM 和 FR 等网络技术,就会发现 IP 网络在设计上存在的不足或缺陷。TCP/IP 通信协议自 20 世纪 60 年代末诞生以来,已经历了 30 多年的实践检验,并成为 Internet 的基础。TCP/IP 通信协议的不断发展和完善促进了 Internet 的发展,同时 Internet 的发展又进一步扩大了 TCP/IP 通信协议的影响。目前,几乎所有厂商的网络产品都支持 TCP/IP,如硬件厂商 Cisco、IMB 等,数据库 Oracle 等,操作系统 NetWare 等。虽然 TCP/IP 取得了巨大的成功,但其存在的设计缺陷不可回避。分析目前广泛使用的 IPv4 协议,在应用中主要存在以下的安全问题。

1. 协议本身的不安全性

例如,在 TCP/IP 参考模型的传输层提供了 TCP 和 UDP 两种协议(2000 年提出了 SCTP 协议,即流控制传输协议),其中 UDP 本身就是一种不可靠、不安全的协议,而 TCP 当初力求通过三次握手机制保障数据传输的可靠性和安全性,但近年来利用 TCP/IP 三次握手出现的网络攻击现象频繁发生。再如,目前在局域网中泛滥的 ARP 欺骗和 DHCP 欺骗,其根源是这些协议在当初设计时只考虑到了应用,而没有或很少考虑安全。还有,如 DNS、POP3、SMTP 和 SNMP 等应用层的协议几乎都存在安全隐患。

2. 应用中出现的不安全因素

当初,设计 Internet 的前身 ARPAnet 的目的很单纯,根本没有考虑到 Internet 在几十年后会发展为今天这样的现状。最初,在 Internet 上传输的主要是一些以纯代码为主的文

本信息，Internet 主要应用于电子邮件的收发。随后要求在 Internet 传输一些图片和文档。再到后来就出现了多媒体应用，即多媒体网络，要求通过计算机网络能够同时处理和传输文字、音频、视频、图形、图像及动画等多种媒体信息。现在，在 VOD(视频点播)技术得到广泛应用的同时，研究者已开始关注 IPTV(网络电视)、VoIP(网络电话)等基于计算机网络的实时通信技术的应用。回顾计算机网络应用的发展历程，一方面是各种新的应用技术层出不穷，另一方面是 TCP/IP 通信协议等基本架构没有发生变化，而且越来越多的要求更高的应用都要争用有限的网络资源。这时研究者和用户开始发现在解决了应用功能的同时，安全问题随之而来。在这种情况下，像 VPN、IPSec 等安全协议开始出现，力求解决网络应用中存在的安全问题。但现实情况是，随着时间的推移及应用需求的不断发展，新的安全问题又会出现。针对这种现象，究其根源还是 IP 网络自身的缺陷，因为 IP 网络本身就是一个“尽力而为”的不可靠的网络，设计者在设计之初根本没有想到网络会成为今天这种现状，或者说 IP 网络本身就不适合于今天的许多网络应用。然而，当大量的应用强加到网络中的时候，带来的最大问题就是安全。

以 IPv4 为代表的 IP 网络目前遇到的困境与今天的道路交通非常相似。目前许多城市的道路还是几年前甚至是几十年前根据当时的交通需求而建设的，但最近几年来交通工具的快速发展导致交通堵塞和交通事故频繁发生。现代社会生活又离不开这些交通工具，所以只能在忍受交通堵塞带来的烦恼的同时，还要解决不断出现和可能遇到的安全问题。

3. 网络基础设施的发展带来的不安全因素

从应用的角度来看，早期的计算机网络多为有线网络。近年来，在铜缆、光纤等有线网络得到大量应用的同时，基于微波、无线电和红外线等无线介质的无线通信方式得到了快速发展，并逐步实现了与有线网络的融合。

从另外一个角度来看，早期计算机网络的应用有其局限性，主要供单位内部的近距离通信。后来，计算机网络的应用逐渐延伸到整个通信领域，通信方式从模拟到数字的转换已成为现实。今天，无论是计算机网络还是电信网络，不管是固定通信还是移动通信，已基本实现了全网的数字化。目前正在推广的 3G 网络，优于以前通信方式的最大特点是数字化和通信速度。但即将制订的 4G 通信标准，开始将无线局域网(Wireless LAN，WLAN)技术与移动通信技术进行融合，使终端的动态连接速率达到 100Mb/s，静态连接速率达到 1Gb/s。

在计算机网络技术的发展过程中，虽然针对有线网络的窃听和物理接入等不安全因素一直存在，但与今天无线通信中所存在和将要面对的安全问题相比，有线通信中存在的安全问题相对要少得多。然而，有线与无线的融合已成为不争的事实，所以随着网络基础设施的不断发展，出现更多的安全问题也是一个不争的事实。

1.1.2 Internet 应用的快速发展带来的安全问题

Internet 由创建于 1969 年的 ARPAnet(Advance Research Projects Agency Network)发展而来，ARPAnet 是由美国国防部出资兴建的，设计 ARPAnet 的最初目的是使各地研究人员在合作一个项目时能快速、灵活地共享代码和信息。当初所连接的节点数只有 4 个，所连接的是大型计算机，当时还没有今天的个人计算机和局域网。在网络中传输的主要是文本信息，数据量较少，应用非常单一。1980 年，ARPAnet 的所有主机都开始采用 TCP/IP 通信协议。在这种情况下，ARPAnet 很少考虑其安全问题。

1983 年，在 ARPAnet 向 TCP/IP 的转换全部结束的同时，美国国防部国防通信局将 ARPAnet 分解成两部分：一部分供民用，名称仍然使用 ARPAnet，另一部分供军方的非机密通信使用，称为 MILnet。随着 TCP/IP 协议的标准化，ARPAnet 的规模不断扩大，不仅美国国内有很多网络与 ARPAnet 连接，许多国家也通过远程通信线路将本地的计算机与网络接入 ARPAnet，成为今天 Internet 的雏形。

Internet 出现后，使用者主要是一些高校和科研院所的学者，主要用于科学研究和学术领域。但到了 20 世纪 80 年代末至 90 年代初期，Internet 的商业应用快速发展，各个公司逐渐意识到 Internet 在产品推销、信息传播及商品交易等方面的价值。Internet 的商业应用，致使用户数量不断增加、应用不断扩展、新技术不断出现、Internet 的规模不断扩大，使 Internet 几乎深入到社会生活的每一个角落。在这种情况下，由于 Internet 本身存在的缺陷及 Internet 商业化带来的各种利益驱动，Internet 上各种攻击和窃取商业信息的现象频繁发生，网络安全问题日益明显。

为此，可以将网络安全的动因主要归纳为三个方面：一是技术缺陷，该缺陷是 IP 网络与生俱来的，而且在今天的 IPv4 网络中更为明显；二是经济利益所驱，由于 Internet 的商业化及其效应不断显现，不法者开始利用 Internet 窃取个人或企业的信息，并从中非法获得经济利益，成为目前 Internet 和 Intranet 上的最大安全风险。例如，2006 年 10 月在 Internet 上广泛传播的“熊猫烧香病毒”，通过盗取用户的 QQ 和游戏账号并从中获利；三是利用 Internet 炫耀个人才能，有些病毒、木马或攻击软件的开发者，其目的并不是为了进行破坏或取得经济利益，而是为了显示自己的计算机专业水平。例如，“硬盘终结者”病毒在发作时将弹出一个信息分析窗口，作者以此来炫耀自己的技术，并希望业内的病毒作者能与其合作。

1.2 网络安全的概念

安全的意义是将资源可能受到的威胁降到最低程度。随着计算机网络的不断发展，全球信息化已成为人类社会发展的大势所趋。但是，由于计算机网络具有连接形式多样、终端分布不均匀、网络系统开放及不同设备之间互连等特征，致使网络易受黑客、恶意软件和其他非法行为的攻击，所以网上信息的安全和保密已成为一个至关重要的问题。对于像银行系统等传输敏感数据的计算机网络系统而言，其网上信息的安全和保密显得尤为重要，因此这些网络必须具有足够强的安全措施。无论是在局域网还是在广域网中，都存在着自然和人为等诸多因素的脆弱性和潜在威胁，因此网络的安全措施应是能全方位地应对各种不同的威胁和脆弱性，这样才能确保网络信息的保密性、完整性和可用性。

国际标准化组织（ISO）对计算机系统安全的定义是：为数据处理系统建立和采用的技术和管理的安全保护，保护计算机硬件、软件和数据不因偶然和恶意的原因遭到破坏、更改和泄露。由此可以将计算机网络的安全理解为：通过采用各种技术和管理措施，使网络系统正常运行，从而确保网络数据的可用性、完整性和保密性。所以，建立网络安全保护措施的目的是确保经过网络传输和交换的数据不会发生增加、修改、丢失和泄露等现象。具体来讲，网络安全包括以下 5 个基本要素。

（1）机密性。确保信息不暴露给未经授权的人或应用进程。

(2) 完整性。只有得到允许的人或应用进程才能修改数据,并且能够判别出数据是否已被更改。

(3) 可用性。只有得到授权的用户在需要时才可以访问数据,即使在网络被攻击时也不能阻碍授权用户对网络的使用。

(4) 可控性。能够对授权范围内的信息流向和行为方式进行控制。

(5) 可审查性。当网络出现安全问题时,能够提供调查的依据和手段。

1.3 网络安全威胁的类型

网络安全威胁指网络中对存在缺陷的潜在利用,这些缺陷可能导致信息泄露、系统资源耗尽、非法访问、资源被盗、系统或数据被破坏等。针对网络安全的威胁来自许多方面,并且会随着技术的发展不断变化。

1.3.1 物理威胁

物理安全是一个非常简单的概念,即不允许其他人拿到或看到不属于自己的东西。目前,计算机和网络中所涉及的物理威胁主要有以下几个方面。

(1) 窃取。包括窃取设备、信息和服务等。

(2) 废物搜寻。是指从已报废的设备(如废弃的硬盘、软盘、光盘和 U 盘等介质)中搜寻可利用的信息。

(3) 间谍行为。是指采取不道德的手段来获取有价值的信息的行为。例如,直接打开别人的计算机复制所需要的数据,或利用间谍软件入侵他人的计算机来窃取信息等。

(4) 假冒。指一个实体假扮成另一个实体后,在网络中从事非法操作的行为。这种行为对网络数据构成了巨大的威胁。

另外,像电磁辐射或线路干扰也属于物理威胁的范围。

1.3.2 系统漏洞威胁

系统漏洞是指系统在方法、管理或技术中存在的缺点(通常称为 bug),而这个缺点可以使系统的安全性降低。目前,系统漏洞主要包括提供商造成的漏洞、开发者造成的漏洞、错误的配置及策略的违背所引发的漏洞等。因此漏洞是方法、管理和技术上存在缺陷所造成的。目前,由系统漏洞所造成的威胁主要表现在以下几个方面。

(1) 不安全服务。指绕过设备的安全系统所提供的服务。由于这种服务不在系统的安全管理范围内,所以会对系统的安全造成威胁。主要有网络蠕虫等。

(2) 配置和初始化错误。指在系统启动时,其安全策略没有正确初始化,从而留下了安全漏洞。例如,在木马程序修改了系统的安全配置文件时就会发生此威胁。

1.3.3 身份鉴别威胁

所谓身份鉴别是指对网络访问者的身份(主要有用户名和对应的密码等)真伪进行鉴别。目前,身份鉴别威胁主要包括以下几个方面。

(1) 口令圈套。常用的口令圈套是通过一个编译代码模块实现的。该模块是专门针对某一些系统的登录界面和过程而设计的,运行后与系统真正的登录界面完全相同。该模块

一般会插入到正常的登录界面之前，所以用户先后会看到两个完全相同的登录界面。一般情况下，当用户进行第一次登录时系统会提示登录失败，然后要求重新登录。其实，第一次登录的用户名和密码并未出错（除非真的输入有误），而是一个圈套，它会将正确的登录数据写入到数据文件中。

（2）口令破解。这是最常用的一种通过非法手段获得合法用户名和密码的方法。

（3）算法考虑不周。密码输入过程必须在满足一定的条件下才能正常工作，这个过程通过某些算法来实现。在一些攻击入侵方法中，入侵者采用超长的字符串来破坏密码算法，从而成功地进入系统。

（4）编辑口令。编辑口令需要依靠操作系统的漏洞，如为部门内部的人员建立一个虚设的账户，或修改一个隐含账户的密码，这样任何知道这个账户（指用户名和对应的密码）的人员便可以访问该系统。

1.3.4 线缆连接威胁

线缆连接威胁主要指借助网络传输介质（线缆）对系统造成的威胁，主要包括以下几个方面。

（1）窃听。是使用专用的工具或设备，直接或间接截获网络上的特定数据包并进行分析，进而获取所需的信息的过程。窃听一般要将窃听设备连接到通信线缆上，通过检测从线缆上发射出来的电磁波来获得所需要的信号。解决该数据被窃听的有效手段是对数据进行加密。

（2）拨号进入。指利用调制解调器等设备，通过拨号方式远程登录并访问网络。当攻击者已经拥有目标网络的用户账户时，就会对网络造成很大的威胁。

（3）冒名顶替。指通过使用别人的用户账户和密码获得对网络及其数据、程序的使用能力。由于别人的用户账户和密码不易获得，所以这种方法实现起来并不容易。

1.3.5 有害程序威胁

计算机和网络中的有害程序是有相对性的，有些有害程序不是出于恶意目的，但却被恶意利用。有害程序造成的威胁主要包括以下几个方面。

（1）病毒。计算机病毒是一个程序，是一段可执行的代码。就像生物病毒一样，计算机病毒有独特的复制能力。计算机病毒可以很快地蔓延，又常常难以根除。它们能把自身附着在各种类型的文件上，当文件在不同的计算机或存储设备之间被复制时，它们就随同文件一起蔓延开来。

（2）逻辑炸弹。逻辑炸弹是嵌入在某个合法程序里面的一段代码，被设置成当满足某个特定条件时就会发作。逻辑炸弹具有病毒的潜伏性。一旦条件成熟导致逻辑炸弹爆发，就会改变或删除数据或文件，引起机器关机或完成某种特定的破坏性操作。

（3）特洛伊木马。特洛伊木马是一个包含在合法程序中的非法程序。该非法程序被用户在不知情的情况下被执行。一般的木马都有客户端和服务器端两个执行程序，其中客户端程序是攻击者进行远程控制的程序，而服务器端程序即是木马程序。攻击者如果要通过木马攻击某个系统，其先决条件是要把木马的服务器端程序植入到要控制的计算机中。

（4）间谍软件。是一种新的安全威胁，它可能在浏览网页或者安装软件时，在不知情的

情况下被安装到计算机上。间谍软件一旦安装就会监视计算机的运行，窃取计算机上的重要信息或者记录计算机的软件、硬件设置，严重危害到计算机中的数据和个人隐私。

1.4 安全策略和安全等级

在现实应用中，没有绝对意义上的安全网络存在。对于一个网络来说，在安全方面要做的首要工作便是制定一个合理可行的安全策略，并根据不同的应用需求制订安全等级和规范。

1.4.1 安全策略

制定安全策略是一件非常复杂的事情，通常可从以下两个方面来考虑。

1. 物理安全策略

物理安全策略包括以下几个方面。

(1) 为了保护计算机系统、网络服务器和打印机等硬件实体和通信链路，以免受自然灾害、人为破坏和搭线攻击。

(2) 验证用户的身份和使用权限，防止用户越权操作。

(3) 确保计算机系统有一个良好的电磁兼容工作环境。

(4) 建立完备的安全管理制度，防止非法进入计算机控制室和各种偷窃、破坏活动的发生。

2. 访问控制策略

访问控制是对要访问系统的用户进行识别，并对访问权限进行必要的控制。访问控制策略是维护计算机系统安全、保护其资源的重要手段。访问控制的内容有入网访问控制、目录级安全控制、属性安全控制、网络服务器安全控制、网络监测和锁定控制、网络端口和节点的安全控制等。另外，还有加密策略、防火墙控制策略等。

1.4.2 安全性指标和安全等级

制定安全策略时，往往需要在安全性和可用性之间采取一个折衷的方案，重点保证一些主要安全性的指标，如下面的安全性指标：

- 数据完整性。在传输过程中，数据是否保持完整。
- 数据可用性。在系统发生故障时，数据是否会丢失。
- 数据保密性。在任何时候，数据是否有被非法窃取的可能。

1985 年 12 月，由美国国防部公布的美国可信计算机安全评价标准(Trusted Computer System Evaluation Criteria，TCSEC)，是计算机系统安全评估的第一个正式标准，该标准最初只是军用标准，后来延至民用领域。TCSEC 将计算机系统的安全划分为 4 个等级 7 个级别。

(1) D 类安全等级。只包括 D1 一个级别。D1 的安全等级最低，D1 系统只为文件和用户提供安全保护。D1 系统最普通的形式是本地操作系统，或者是一个完全没有保护的网络。DOS 和 Windows 95/98 操作系统的安全等级属于 D1 级。

(2) C 类安全等级。该类安全等级能够酌情提供安全保护，并为用户的行动和责任提

供审计能力。C类安全等级可划分为C1和C2两类,其中C1系统的可信任运算基础体制(Trusted Computing Base,TCB)通过将用户和数据分开来达到安全的目的。在C1系统中,所有的用户以同样的灵敏度来处理数据,即用户认为C1系统中的所有文档都具有相同的机密性。C2系统比C1系统加强了可调的酌情控制。在连接到网络上时,C2系统的用户分别对各自的行为负责。C2系统通过登录过程、安全事件和资源隔离来增强这种控制。C2系统具有C1系统中所有的安全性特征。Unix、NetWare3.x及以上版本及Windows NT的安全等级为C2级。

(3) B类安全等级。分为B1、B2和B3三类,其中B类系统具有强制性保护功能。强制性保护意味着如果用户没有与安全等级相连,系统就不会让用户访问对象。其中,B1系统满足下列要求:系统对网络控制下的每个对象都进行灵敏度标记;系统使用灵敏度标记作为所有强迫访问控制的基础;系统在把导入的、非标记的对象放入系统前标记它们;灵敏度标记必须准确地表示其所联系对象的安全级别;当系统管理员创建系统或者增加新的通信通道或I/O设备时,管理员必须指定每个通信通道和I/O设备是单级还是多级,并且管理员只能手工改变指定;单级设备并不保持传输信息的灵敏度级别;所有直接面向用户位置的输出(无论是虚拟的还是物理的)都必须产生标记来指示关于输出对象的灵敏度;系统必须使用用户的口令或证明来决定用户的安全访问级别;系统必须通过审计来记录未授权访问的企图。

B2系统必须满足B1系统的所有要求。另外,B2系统的管理员必须使用一个明确的、文档化的安全策略模式作为系统的可信任运算基础体制。B2系统必须满足下列要求:系统必须立即通知系统中的每一个用户所有与之相关的网络连接的改变;只有用户能够在可信任通信路径中进行初始化通信;可信任运算基础体制能够支持独立的操作者和管理员。

B3系统必须符合B2系统的所有安全需求。B3系统具有很强的监视委托管理访问能力和抗干扰能力。B3系统必须设有安全管理员。B3系统应满足以下要求:除了控制对个别对象的访问外,B3必须产生一个可读的安全列表;每个被命名的对象提供对该对象没有访问权的用户列表说明;B3系统在进行任何操作前,要求用户进行身份验证;B3系统验证每个用户,同时还会发送一个取消访问的审计跟踪消息;设计者必须正确区分可信任的通信路径和其他路径;可信任的通信基础体制为每一个被命名的对象建立安全审计跟踪;可信任的运算基础体制支持独立的安全管理。

(4) A类安全等级。A系统的安全级别最高。目前,A类安全等级只包含A1一个安全类别。A1类与B3类相似,对系统的结构和策略不作特别要求。A1系统的显著特征是,系统的设计者必须按照一个正式的设计规范来分析系统。对系统分析后,设计者必须运用核对技术来确保系统符合设计规范。A1系统必须满足下列要求:系统管理员必须从开发者那里接收到一个安全策略的正式模型;所有的安装操作都必须由系统管理员进行;系统管理员进行的每一步安装操作都必须有正式文档。

1.5 常用的网络安全管理技术

针对以上所提到的网络安全问题,为了保护网络信息的安全可靠,在运用法律和管理手段的同时,还需要依靠相应的技术来加强对网络的安全管理。

1.5.1 物理安全技术

物理安全，是保护计算机网络设备、设施及其他介质免遭地震、水灾和火灾等环境事故，以及人为操作失误及各种计算机犯罪行为导致破坏的过程，主要包括环境安全、设备安全和介质安全三个方面。

保证物理安全可用的技术手段很多，这方面有许多可以依据的标准。例如，国家标准GB50173-93《电子计算机机房设计规范》、国家标准GB2887-89《计算站场地技术条件》、GB9361-88《计算站场地安全要求》，以及其他诸如防辐射、防电磁干扰的众多标准等。当然，要保证物理安全，人员素质管理也非常重要。一方面需要制定切实可行的安全管理制度，另一方面需要加强对人员安全意识的教育和培养。

1.5.2 安全隔离

传统的以太网络，信息发送采用的是广播方式，实际上就给信息“共享”打开了通道。恶意攻击者只要能够进入局域网，就可能监听所有数据通信，窃取机密。

1. 安全隔离的概念

随着新型网络攻击手段的不断出现和一些企事业单位对网络安全要求的不断提高，一个全新的概念——“安全隔离技术”应运而生。安全隔离技术的目标是在确保把有害攻击隔离在可信网络之外，并保证可信网络内部信息不外泄的前提下，完成不同网络之间信息的安全交换和共享。到目前为止，安全隔离技术已经过了以下几个发展阶段。

(1) 完全隔离。采用完全独立的设备、存储和线路来访问不同的网络，做到了完全的物理隔离，但需要多套网络和系统，建设和维护成本较高，一般仅适用于一些专用网络。目前，像公安系统的公安专网、军队系统的军网等专用网络便是采用安全隔离方式来实现的。

(2) 硬件卡隔离。通过硬件卡控制独立存储和分时共享设备与线路来实现对不同网络的访问。该技术在20世纪90年代中期应用较为广泛，许多政府机关和企事业单位为了保护计算机上的数据，多采用硬件卡进行隔离。因为在此期间，多数计算机仍以单机操作为主，当需要上网时，则通过硬件卡切换到另一系统，以加强对系统数据资源的保护。目前，该技术仍然在一定范围内使用，但存在使用不便、可用性差等问题，有些还存在设计上的安全隐患。

(3) 数据转播隔离。利用转播系统分时复制文件的途径来实现隔离。该方法切换时间较长，甚至需要手工完成，不仅大大降低了访问速度，更不支持常见的网络应用，只能完成特定的基于文件的数据交换。

(4) 空气开关隔离。该技术是通过使用单刀双掷开关，通过内外部网络分时访问临时缓存器来完成数据交换的。该方法支持的网络应用较少，传输速度慢，硬件故障率较高，容易成为网络的瓶颈。

(5) 安全通道隔离。该技术通过专用通信硬件和专有交换协议等安全机制，来实现网络间的隔离和数据交换。不仅解决了以往隔离技术存在的问题，并且在网络隔离的同时实现高效的内外网数据的安全交换，它透明地支持多种网络应用，成为当前隔离技术的发展方向。

2. 网络分段

网络分段是保证网络安全的一项基本措施，其宗旨是根据业务或分类级别的不同，将网络和用户分类隔离。通过设定不同的权限控制，防止越级越权对网络资源的非法访问。

网络分段有物理分段和逻辑分段两种方式。其中，物理分段通常是指将网络从物理层和数据链路层上分为若干网段，各网段之间无法进行直接通信。目前，许多交换机都有一定的访问控制能力，可实现对网络的物理分段。逻辑分段则是指将整个系统在网络层上进行分段，对于 TCP/IP 网络，可以根据 IP 地址将网络分成若干子网，各子网间必须通过可路由的网关设备（三层交换机或路由器）进行连接，并通过这些设备自身的安全机制（如 ACL、QoS 等）来控制各子网间的相互访问。逻辑分段应用灵活，适用范围广，是目前研究和应用的主要领域。

1.5.3 访问控制

访问是使信息在不同设备之间流动的一种交互方式。访问控制决定了谁能够访问系统，能访问系统的何种资源及如何使用这些资源。适当的访问控制能够阻止未经允许的用户有意或无意地获取数据。访问控制的手段包括用户识别代码、口令、登录控制、资源授权（例如用户配置文件、资源配置文件和控制列表）、授权核查、日志和审计。

访问控制主要是通过防火墙、交换机或路由器的使用来实现的。防火墙是实现网络安全最基本、最经济、最有效的安全措施之一，通过制定严格的安全策略，防火墙可以对内外网络或内部网络不同信任域之间进行隔离，使所有经过防火墙的网络通信接受设定的访问控制。此外，通过防火墙提供的 NAT 功能，也可以起到网段隔离的作用（主要是局域网与广域网之间）。

另外，随着微电子技术的发展，交换机和路由器的数据处理和存储能力得到了提高。为此，目前许多设备已集成了原来多个设备所提供的功能。例如，现在的绝大多数防火墙已提供了原来路由器才具有的 ACL、NAT 等功能。同时，在一些路由器上也提供了原本由防火墙才具有的访问控制功能。

1.5.4 加密通道

给网络通信提供加密通道，也是普遍使用的一项安全技术。随着技术的发展，目前加密通道可以建立在数据链路层、网络层、传输层甚至是应用层。

1. 数据链路层加密

数据链路层加密可以使用专用的链路加密设备，其加密机制是点对点的加、解密。在通信链路两端，都应该配置链路加密设备，通过位于两端加密设备的协商配合来实现传输数据的加密和解密过程。

近年来，VPN（Virtual Private Network，虚拟专用网）技术得到了快速发展，并得到了广泛应用。其中，位于数据链路层的 VPN 可以实现链路层加密。目前这样的 VPN 技术主要有三种：L2F（Layer 2 Forwarding，第二层转发）、PPTP（Point-to-Point Protocol，点对点隧道协议）和 L2TP（Layer 2 Tunneling Protocol，第二层隧道协议）。在进行网络通信时，链路层 VPN 首先会将各种网络协议封装到 PPP 中，再把整个数据装入隧道协议中。这种双层封装形成的数据包依靠链路层协议来传输，最终起到点对点加密通信的效果。

2. 网络层加密

网络层加密通过网络层 VPN 技术来实现，最典型的就是 IPSec。现在许多提供 VPN 功能的防火墙设备中都支持 IPSec。

网络层 VPN 也需要对原始数据包进行多层封装，但最终形成的数据包是依靠第三层协议（一般是 IP 分组）来进行传输的，本质上是端到端的数据通信。

3. 传输层加密

传输层加密通道可以采用 SSL（Secure Socket Layer，安全套接层）和 TLS（Transport Layer Security，传输层安全）技术。SSL 是应用比较广泛的一种传输层安全协议，它介于应用层协议和 TCP/IP 之间，为传输层提供安全性保证。

TLS 是 IETF 的标准，它建立在 SSL 3.0 基础之上，只是所支持的加密算法不同，这两种加密协议不能互通。

此外，还有一些其他的传输层安全技术，例如 SSH、SOCKS 等。

4. 应用层加密

应用层加密与具体的应用类型结合紧密，典型的有 SHTTP、SMIME 等。安全超文本传输协议（Secure HyperText Transfer Protocal，SHTTP）是面向消息的安全通信协议，可以为单个 Web 主页定义加密安全措施。而 SMIME（Secure Multipurpose Internet Mail Extensions，加密多用途 Internet 邮件扩展）则是一种电子邮件加密和数字签名技术。应用层加密还包括利用各种加密算法开发的加密程序。

1.5.5 入侵检测

入侵检测（Intrusion Detection）技术是近年来发展迅速的一种安全技术。我们知道，防火墙是最早被采用的访问控制措施，但由于防火墙“防外不防内”的先天性弱点，加上防火墙对实时入侵行为识别及反应能力的限制，使得入侵检测技术成为整体安全解决方案中必不可少的一部分。

入侵检测技术，即通过在计算机网络或计算机系统的关键点采集信息进行分析，从中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象。入侵检测所使用的软件与硬件的组合便是入侵检测系统（IDS）。

根据检测对象的不同，可将入侵检测系统分为两类：基于主机的入侵检测系统（HIDS）和基于网络的入侵检测技术（NIDS）。

NIDS 是最常使用的一种入侵检测系统，它作为共享网络中的一个节点，对本网段上的通信数据进行侦听，这种采集数据的方法就是典型的 Sniffer 技术，通过对网络中通信数据的分析，发现其中的可疑痕迹。一般情况下，NIDS 对入侵行为的检测多是通过模式匹配来进行的。也就是说，选择某种匹配算法，将获得的数据信息与规则库（漏洞库）中的模式进行比较，从中发现已知的攻击行为。这种入侵检测系统不需要主机提供严格的审计，对主机资源消耗少，并可以提供对网络通常的保护而无需顾及复杂网络中异构主机的特殊情况。当然，误报（false positive）和漏报（false negtive）往往是 NIDS 存在的最大问题。此外，NIDS 并不能对主机内部的活动进行检测，这无疑会使入侵检测的成效受影响。

HIDS 通过提取并分析主机的审计记录（日志）来检测入侵。这种入侵检测系统和主机结合紧密，往往需要根据不同类型的主机系统采用不同的检测方法。另外，它的实时性比较

差，通常可以作为事后追查入侵者并提取证据的一种手段。

IDS技术发展到现在，已经出现了许多种检测方法，从最初的模式匹配和审计方法，到基于统计和专家系统、原型系统的方法，也有基于移动代理技术的检测方法。此外，IDS的整体构架也有所扩展，单一布局的IDS结构已经不适应多网段入侵检测的要求，分布式、多系统的IDS将是一个重点发展的方向。

1.5.6 入侵保护

安全防护是一个多层次的保护机制，它既包括企业的安全策略，又包括防火墙、防病毒和入侵检测等产品技术解决方案。而且，为了保障网络安全，还必须建立一套完整的安全防护体系，进行多层次、多手段的检测和防护。其中，IDS正是构建安全防护体系不可缺少的一个环节。促使IDS得到广泛应用的一个因素是Slammer、冲击波等针对系统漏洞的攻击不断增多，新的软件漏洞不断被发现，一些分析系统缺陷、编写攻击程序或制作蠕虫病毒的简单工具也在不断发展之中，从发现缺陷到释放出蠕虫病毒的时间间隔进一步缩短，用户需要一种可以检测攻击的有效工具，IDS就是其中的一种。

近年来，IDS在网络中的应用日渐增多，尤其在对安全等级要求较高的证券、金融及电信的网络中，IDS的应用非常普及，不过IDS所带来的麻烦也越来越明显。例如，IDS的误报率太高，在每天发出的大量报警信息中，真正有价值的信息却寥寥无几，而从大量信息中筛选出有用信息不是一件容易的事情。另外，许多用户希望IDS能够增加主动阻断攻击的能力，在危害出现时能够直接将其阻断，而不是让其进入网络。在Windows操作系统普遍使用的今天，操作系统漏洞屡屡成为被攻击的依据，主动防御和应用安全的压力将显得更为突出。一方面，系统的复杂性在不断提高，几乎每周都会有系统缺陷被发现；另一方面，利用高危缺陷进行入侵和传播的攻击技术也在快速发展，用户需要一种能够实时阻断攻击的安全技术。

从技术上看，IPS(Intrusion Prevention System，入侵保护系统)和IDS之间有着必然联系，IPS可以被看作是增加了主动阻断功能的IDS。但是，IPS绝不仅仅是增加了主动阻断的功能，而是在性能和数据包的分析能力方面都比IDS有了质的提升。

由于增加了主动阻断能力，检测准确程度的高低对于IPS来说十分关键。除了检测机制外，IPS的检测准确率还依赖于应用环境。一些流量对于某些用户来说可能是恶意的，而对于另外的用户来说就是正常流量，这就需要IPS能够针对用户的特定需求提供灵活而易用的策略，以提高检测准确率。引入弱点分析技术是IPS的另一个亮点，IPS厂商通过分析系统漏洞、收集和分析攻击代码或蠕虫代码、描述攻击特征或缺陷特征，使IPS能够主动保护脆弱系统。

绝大多数IDS系统都是被动的，而不是主动性的。在攻击实际发生之前，IDS往往无法预先发出警报。IPS则倾向于提供主动性的防护，其设计旨在预先对入侵活动和攻击性网络流量进行拦截，避免其造成任何损失，而不是简单地在恶意流量传送时或传送后才发出警报。IPS是通过直接嵌入到网络流量中而实现这一功能的，即通过一个网络端口接收来自外部系统的流量，经过检查确认其中不包含异常活动或可疑内容后，再通过另外一个端口将它传送到内部系统中。这样一来，有问题的数据包，以及所有来自同一数据流的后续数据包，都能够在IPS设备中被清除掉。

在主动防御渐入人心之时,IDS 的报警功能仍是主动防御系统所必需的。也许 IDS 的产品形式会消失,但是 IDS 的检测功能并不会因形式的消失而消失,只是逐渐被转化和吸纳到其他的安全设备当中。但在实际应用中,由于 IPS 的许多技术目前并没有取得业界的公认,所以 IDS 在短期内还不会消亡,同时 IPS 也不会完全取代 IDS 的作用。

1.5.7 安全扫描

前面所介绍的安全技术多是被动的防御,如果要真正了解网络当前的安全状况,就应该采用安全扫描技术,对网络整体的安全状况进行有效评估。实事上,在网络安全建设周期中,安全评估应该是一个很重要的环节。

进行网络安全扫描,选择合适的工具是个关键。一般来讲,扫描工具可以分为基于网络的扫描器和基于主机的扫描器。其中,基于网络的扫描器可以置于网络的任何部位,可以从外部网络透过防火墙对内部网络进行扫描,也可以在内部网络直接对网络中的主机和设备进行扫描。这种工具的使用非常灵活,它可以完全模拟黑客的入侵和攻击行为,对网络的安全状况进行最直接的评测。其效果如何,基本上取决于扫描规则的完备和更新程度。

基于主机的扫描器一般采用 Agent/Console(代理/控制台)结构,通常是一对一的单点扫描。在要扫描的目标主机上安装代理程序,由代理程序完成真正的扫描工作,而控制台负责向代理发送扫描指令,并汇总分析扫描结果。因为代理直接在目标主机上运行,所以可以对主机进行更细致、更全面的检测,一般还具有日志审计功能。

无论哪种扫描工具,对扫描规则库进行及时更新应该是起码的要求。当然,扫描工具提供的最终结果报告也应该具有多样性,以满足人们的不同需求。

1.5.8 蜜罐技术

蜜罐(honeypot)是一种计算机网络中专门为吸引并“诱骗”那些试图非法入侵他人计算机系统的人而设计的“陷阱”系统。

1. 蜜罐的概念和作用

蜜罐是一种被侦听、被攻击或已经被入侵的资源,使用和配置蜜罐的目的是使系统处于被侦听、被攻击状态。蜜罐组织的专家 L. Spitzner 对蜜罐的定义为:蜜罐是一种资源,它的价值是被攻击或攻陷。这就意味着蜜罐是用来被探测、被攻击甚至最后被攻陷的,蜜罐不会修补任何东西,这样就为使用者提供了额外的、有价值的信息。蜜罐不会直接提高计算机网络安全,但它却是其他安全策略所不可替代的一种主动攻击技术。

蜜罐并非一种安全解决方案,因为蜜罐并不会对产生的侦听、攻击等行为采取任何阻止手段。蜜罐只是一种工具,是对系统和应用的仿真,可以创建一个能够将攻击者困在其中的环境。蜜罐技术已经发展成为诱骗攻击者的一种非常有效而实用的方法,它不仅可以转移入侵者的攻击,保护用户的主机和网络不受入侵,而且可以为入侵的取证提供重要的线索和信息。

蜜罐技术已经被广泛应用于因特网的安全研究中。对于一个安全研究组织来说,面临的最大问题是缺乏对入侵者的了解。他们最需要了解的是谁正在攻击、攻击的目的是什么、攻击者如何进行攻击、攻击者使用什么方法进行攻击及攻击者何时进行攻击等。目前解决这些问题的最好方法之一是蜜罐技术。蜜罐可以为安全专家们提供一个学习各种攻击的平

台。在研究攻击入侵中,没有其他方法比观察入侵者的行为并一步步记录攻击过程直至整个系统被入侵更具有应用价值。

蜜罐是一个可以模拟具有一个或多个攻击弱点的主机系统,为攻击者提供一个易于被攻击的目标。蜜罐中所有的假终端、子网等都经过设计人员的精心策划,以吸引攻击者的攻击。例如,蜜罐设计人员可以在因特网上定义这样一台主机,其主机名为 www.bank.com.cn,并在该系统中提供一些让攻击者可以很容易猜测到的用户账户。当攻击者闯入系统时,对进行的操作进行记录,并收集相关的数据。这些数据是分析网络安全的最好资料。

2. 蜜罐的分类

蜜罐可以分为牺牲型蜜罐、外观型蜜罐和测量型蜜罐三种基本类型。

(1) 牺牲型蜜罐。是一台简单的为某种特定攻击设计的计算机。牺牲型蜜罐一般放置在易受攻击的地点,并假扮为攻击的受害者,为攻击者提供极好的攻击目标。牺牲型蜜罐的不足是提取攻击数据比较难,而且本身也会被攻击者利用来攻击其他的主机。

(2) 外观型蜜罐。仅对网络服务进行仿真,而不会导致主机真正被攻击,从而蜜罐的安全不会受到威胁。研究人员对外观型蜜罐中记录的数据的访问更加方便,可以更容易地检测到攻击者。外观型蜜罐是一种最简单的蜜罐,通常由某些应用服务的仿真程序构成。外观型蜜罐也具有与牺牲型蜜罐相同的弱点。

(3) 测量型蜜罐。综合了牺牲型蜜罐和外观型蜜罐的特点,与牺牲型蜜罐类似,测量型蜜罐为攻击者提供了高度可信的系统;与外观型蜜罐类似,测量型蜜罐非常容易访问,但攻击者很难绕过。

目前,成熟的蜜罐产品也比较多,如 DTK(Deception Tool Kit)、BOF(Back Orifice Friendly)、Specter、Home-made 和 Honeyd 等。对网络攻击感兴趣的读者可以选择一款蜜罐产品,研究攻击现象的详细发生过程。

1.5.9 物理隔离技术

目前没有一种技术可以解决所有的安全问题。但是,防御的深度越深,网络就越安全。物理隔离是目前能够较好地解决各类安全问题的一项技术,它是近年来出现的一个全新的安全防御手段,解决了许多高保密单位对于机密信息的安全要求。随着物理隔离技术的日渐完善,物理隔离产品正在逐渐成为网络安全体系中必不可少的环节之一。

1. 物理隔离的概念

物理隔离技术的基本思想是:如果不存在与网络的物理连接,网络安全威胁便可大大降低。目前,我国有些单位(如政府、证券、部队和银行等)的内部网络上有着大量机密的数据和信息,所以网络安全在这些单位显得非常重要。为了确保内部数据和信息的安全,或者限制接入因特网,或者使用两个完全独立的网络。但事实上,政府、证券、部队和银行等单位不仅要上网,而且还要走在前列。使用两个物理上独立的网络不仅价格昂贵,而且不实用。当涉密网络和非涉密网络之间通过移动介质(如 U 盘、移动硬盘等)进行数据传输时并不安全。我国对计算机信息安全问题已经高度重视,在 2000 年 1 月 1 日起由国家保密局颁布并实施的《计算机信息系统国际联网保密管理规定》第 2 章第 6 条中规定:涉及国家秘密的计算机信息系统,不得直接或间接地与国际互联网或其他公共信息网络相连接,必须实行物理隔离。

物理隔离技术的目的就是实现内外网信息的隔离。实现物理隔离必须保证隔离双方的信息不会出现在同一个存储介质上，彼此信息不会出现在对方的网络中。因此，物理隔离通常存在两个存储介质，而且这两个存储介质在同一时刻只能有一个有效。目前，物理隔离的实现方案通常包括客户端选择设备和网络选择器，用户通过开关设备或通过键盘来控制客户端选择不同的存储介质。

2. 物理隔离的两种类型

物理隔离技术是解决网络安全问题的一种技术。从广义上讲，物理隔离可以分为网络隔离和数据隔离两种类型。

（1）网络隔离。网络隔离就是把被保护的网络从开放、无边界、自由的环境中独立出来。这样，公共网络上的攻击者和计算机病毒将无从入手，保证了被保护系统的安全性。实现网络隔离主要采用两种方式：物理网络隔离和逻辑网络隔离。其中物理网络隔离就是使网络与计算机设备在空间上进行分离，不存在有线或无线的电气连接，它是最直观、简单、可靠的隔离方法。物理网络隔离需要在同一办公室、同一个大楼内组建多个物理网络。逻辑网络隔离一般通过网络设备的功能来实现。例如，目前使用的交换机都支持数据链路层（OSI 参考模型第二层）的 VLAN（虚拟局域网）功能，可实现不同端口之间的逻辑隔离。当在一个二层交换机上划分了多个 VLAN 时，位于不同 VLAN 之间的计算机之间是无法直接通信的，这样便实现了逻辑网络的隔离。

（2）数据隔离。不管网络隔离采用的是物理网络隔离还是逻辑网络隔离，如果在使用中出现一台计算机能够连接两个或两个以上的网络，那么所有的网络隔离也就失去了意义，因为在同一台计算机连接多个网络的过程中没有把存储设备隔离开来。数据隔离是指存储数据的介质只能针对其中的一种网络而存在。

通过以上分析，物理隔离在安全上需要达到以下三点要求。

① 在物理传输上使不同网络之间隔断，确保不同的网络不能通过网络连接而侵入不同的网络。对于使用内外网络的用户，防止内部网络中的数据通过网络连接被泄漏到外部网络。

② 在物理辐射上隔断不同网络，确保不同网络之间不会通过电磁辐射或耦合方式泄漏信息。

③ 在物理存储介质上隔断两个网络环境，对于断电后会遗失信息的部件（如内存、CPU 等），要在网络转换时进行清除处理，防止残留信息出网；对于断电非遗失信息的设备（如硬盘、磁带机等），不同网络的信息应分开存储。

1.5.10 灾难恢复和备份技术

灾难恢复技术，也称为业务连续性技术，是信息安全领域一项重要的技术。它能够为重要的计算机系统提供在断电、火灾等各种意外事故发生时，甚至在如洪水、地震等严重自然灾害发生时保持持续运行的能力。对企业和社会关系重大的计算机系统都应当采用灾难恢复技术予以保护。

进行灾难恢复的前提是对数据的备份，之所以要进行数据备份，是因为现实生活中有种种人为或非人为因素造成的意外的或不可预测的灾难发生，其中包括计算机或网络系统的软硬件故障，人为操作故障，资源不足引发的计划性停产，生产场地的灾难。

传统的备份技术，主要采用主机内置或外置的磁带机对数据进行冷备份，这种方法在数据量不大、操作系统种类单一、服务器数量有限的情况下，不失为一种既经济又简单的备份手段。但随着企业计算机系统规模的扩大、数据量几何级的增长，以及分布式网络环境的兴起，企业将越来越多的业务分布在不同的机器、不同的操作平台上，这种单机的人工冷备份方式已不再适应新的需求。

一个好的备份系统应该是全方位、多层次的，它应该具有下列特点。

（1）集中式管理。

（2）自动化的备份。

（3）对大型数据库的备份和恢复。

（4）具备较强的备份索引功能。

（5）归档管理。

（6）系统灾难恢复。

（7）具有较好的可扩展性。

一个完整的备份及灾难恢复方案，应该包括备份硬件、备份软件、备份制度和灾难恢复计划 4 个部分。选用了先进的备份硬件后，绝不能忽略备份软件的选择，因为只有优秀的备份软件才能充分发挥硬件的先进功能，保证快速、有效的数据备份和恢复。此外，还需要根据企业自身情况制定日常备份制度和灾难恢复计划，并由管理人员切实执行备份制度，否则系统安全将仅仅是纸上谈兵。

目前许多大的 IT 厂商都提供有完整的备份及灾难恢复解决办法，例如，IBM 的 SSA 磁盘系统、Magstar 磁带系统、ADSM 存储管理软件，惠普的单键灾难恢复技术（OBDR）等，具体选用什么样的产品，还要根据企业的实际需求及当前存储产品的功能特点来决定。

1.6 网络安全管理新技术

大部分网络安全问题是随着网络应用的不断发展而出现的，下面介绍的上网行为管理和 UTM 是目前网络安全管理中两项较新的技术。

1.6.1 上网行为管理

随着以 Internet 为代表的计算机网络的快速发展，如何用好网络资源，使之更好地为用户提供服务，已是刻不容缓的责任和压力。伴随着网络的发展，各种网络犯罪、网络诈骗和有害资源肆意蔓延。员工在上班时间上网聊天、购物和游戏等行为严重影响了工作效率；部分缺乏保密意识的员工则通过 MSN、QQ 等即时通信软件或博客和邮件等方式有意或无意地将组织内部机密信息泄漏；日益流行的 BT、电驴等下载软件非常容易导致关键业务应用系统带宽无法保证。这些现象已严重影响了网络的安全，急需采取相应的措施进行管理。

员工上网行为管理（Employee Internet Management，EIM）为解决上述难题提供了可供选择的方案。EIM 可以为政府监管部门、各行业信息主管部门及企业管理用户提供帮助，能有效平衡员工上网所带来的影响，在开放网络资源的同时，最大限度地保障网络资源不被滥用。

EIM 相关产品和应用已经过了以下几个发展阶段。

- IAC(Internet Access Control,Internet 访问控制)。通过建立企业网络地址数据库,规定哪些网站不能访问,这样可以将禁止访问的几乎大部分网站都被屏蔽,不允许员工在企业网内访问。
- IAM(Internet Access Management,Internet 访问管理)。该阶段属于 Internet 接入管理的初级阶段,以保持企业的工作效率为目的,通过建立相关的 Internet 接入策略和管理功能,对不同人员、不同部门的机构实施上网权限管理和资源分配,并用报表形式系统显示员工访问 Internet 的记录。
- EIM。属于真正的上网行为管理阶段,以提高企业的工作效率为目的,企业不但建立相关上网策略,还进一步与企业信息系统的安全管理结合起来。能够根据用户对象的不同来分配网络资源,并能够建立详细的员工访问 Internet 的日志,提供详细的报表,帮助企业管理层分析员工的上网行为,并对上网的策略进行相关调整。

图 1-1 所示的是某一单位 EIM 系统的部署情况。其中,EIM 的核心设备"网络行为分析系统"可以接入单位的中心交换机,从中心交换机获得网络的流量,再通过"管理控制台"进行实时查看和统计分析。一个完整的 EIM 系统应具有以下功能。

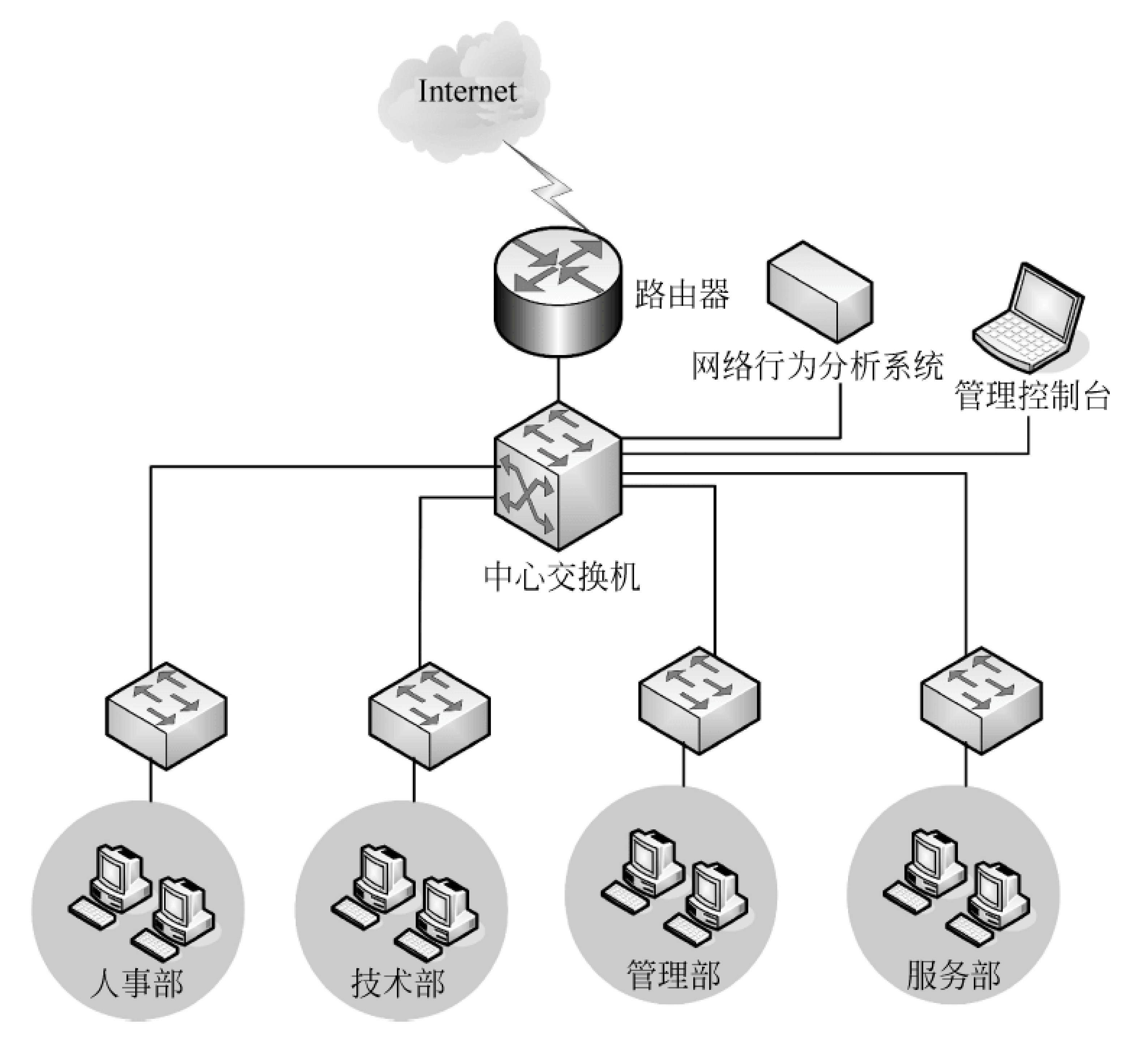


图 1-1 某单位网络行为管理系统网络示意图

(1) 控制功能。可合理分配不同部门、员工的上网权限,如什么时间可以上网、什么时间不能上网,能够访问哪些 Internet 网站的内容,哪些 Internet 资源是严格禁止使用的。另外,还可以对代理软件进行封堵,防止不允许上外网的员工通过代理软件上外网。

(2) 监控与审计功能。可以将所有与上网相关的行为记录下来。例如,对企业研发、财务等关键部门的上网行为、聊天内容和邮件内容进行记录,以便事后审计,并在内部起到威慑的效果。

(3) 报表分析功能。可以方便直观地统计分析员工的上网情况,据此掌握单位内部网络(Intranet)的使用情况。

(4) 流量控制与带宽管理。支持对不同员工进行分组,通过一段时间数据统计,限定每个组的上网流量,对 BT、电驴等 P2P 下载软件进行封堵,避免其对网络带宽资源的消耗。

1.6.2 统一威胁管理

统一威胁管理(Unified Threat Management,UTM)是一种被广泛看好的信息安全解决方案。

1. UTM 的定义

UTM 首先出现在 2003 年 IDC(Internet Data Center,互联网数据中心)的研究报告中。IDC 报告中将 UTM 定义为包括 firewall,intrusion detection and prevention,and gateway anti-virus 的设备。如图 1-2 所示,UTM 是一个以整合式安全设备为代表的安全产品,它包括防火墙、入侵检测与防护(IDS/IPS)及网关防病毒等功能。UTM 是由硬件、软件和网络技术组成的具有专门用途的设备,主要提供一项或多项安全功能,将多种安全特性集成于一个硬件设备里,构成一个标准的统一管理平台。

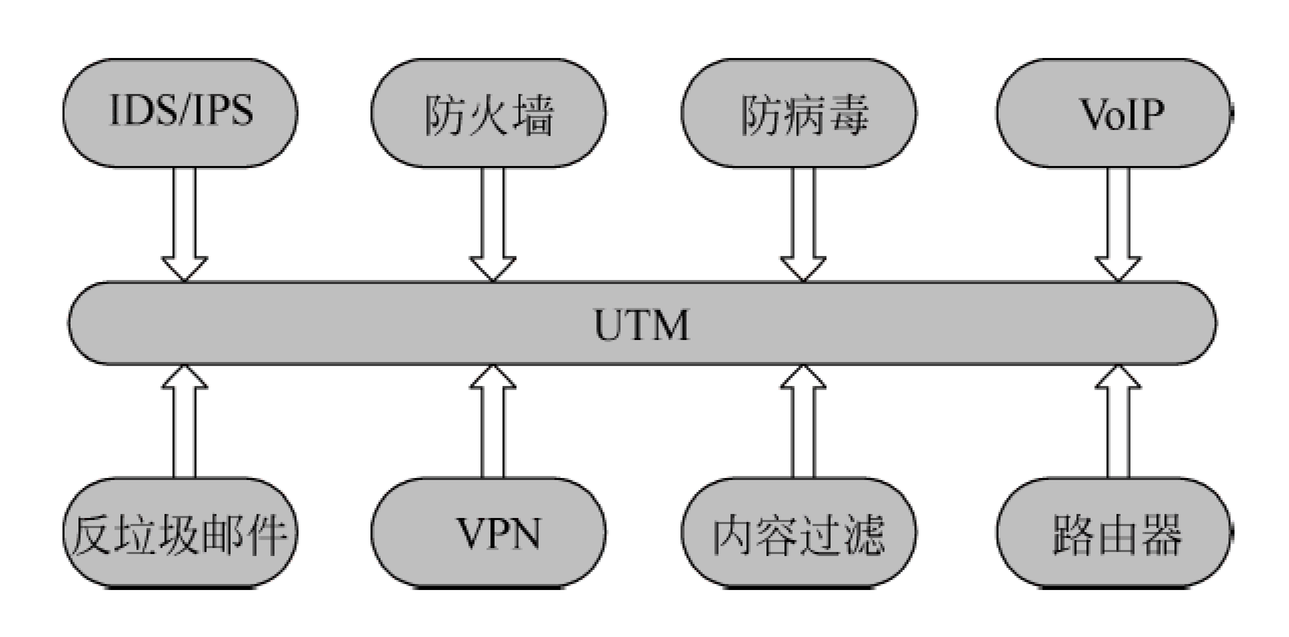


图 1-2　UTM 系统提供的功能

具体来讲,UTM 具有传统的网络防火墙的功能,可以提供防火墙所具有的状态检测、包过滤等基本的安全管理功能。同时提供了网络防御,能够抵御 DoS/DDoS(拒绝服务/分布式拒绝服务)。还可以防御病毒和恶意软件、垃圾邮件及网络钓鱼的攻击。

2. UTM 的功能

UTM 提供了以下功能。

(1) 整合网络安全。在 UTM 概念出现之前,局域网为了防御各种各样的威胁,需要配置多个单功能的安全产品,例如防火墙、防病毒网关、防垃圾邮件系统及 URL 过滤网关等。由于这些安全产品分别由不同的厂商提供,所以管理和维护很不方便。另外,网络中每增加一台设备就会增加一个故障点,不利于系统的安全运行。UTM 的提出解决了局域网络必须管理多个单功能产品的难题。通过单一的操作系统与管理接口,提供一个能够满足多方位安全需求的全功能架构。

(2) 降低技术复杂度。UTM 安全设备中装入了很多功能模块,提高了局域网的易用性。另外,这些功能模块的协同运作无形中降低了掌握和管理各种安全功能的难度,并减少了用户误操作的可能性。

(3) 简化网络管理。UTM 的价值在于简化管理,即以最精简的单一设备来达到所需要

的网络管理水平，并具有快速迁移、集中管理和节省成本的优势。

另外，UTM 产品还具有降低安全管理的复杂度、集成的维护平台、单一服务体系结构、集中的安全日志管理、组合式的安全保护、应用的灵活性、良好的可扩展性及进一步降低成本等优势，为目前流行的安全威胁提供有效的防御机制。

3. UTM 的发展

UTM 设备可说是计算机网络安全解决方案的一个重要突破。综合分析目前网络安全产品的功能，UTM 具有显著的优点，而且相关的技术正在应用中不断发展和完善。现在，UTM 设备已经为用户提供了分层安全(layer security)的功能，它可以与用户计算机上安装的防病毒软件、在防火墙上添加的防毒墙功能配合工作，为用户提供重重防护关卡。另外，现在已经有厂商开始将 VoIP、路由器等功能整合进 UTM 设备中。

随着网络新型应用的不断出现和各种安全威胁的产生，将来 UTM 产品还将融入更多的安全防护功能，并支持各种操作系统。

习　　题

1-1　结合目前网络的应用，简述为什么要研究网络安全。

1-2　计算机网络的不安全性主要由哪些因素引起？如何解决？

1-3　网络安全的概念是什么？

1-4　计算机网络主要存在哪些安全威胁？

1-5　在计算机网络的安全管理中，物理安全策略和访问控制策略有何特点？

1-6　在计算机网络中，常用的安全管理技术有哪些？

1-7　结合单位网络的应用特点，谈谈上网行为管理的重要性。

1-8　什么是 UTM？UTM 在计算机网络安全管理中发挥着什么作用？

1-9　什么是密罐技术？在计算机网络安全研究中蜜罐能够发挥什么作用？

1-10　什么是物理隔离？在计算机网络安全管理中有何意义？

第2章　数据加密技术及应用

数据加密技术是指对在网络中所发送的明文消息用加密密钥加密成密文进行传送，接收方用解密密钥进行解密再现明文消息，从而保证传输过程中密文信息即使被泄漏，在无密钥的情况下仍是安全保密的。目前，数据加密技术已被普遍应用于计算机网络信息的安全管理中。通过本章的学习，读者将对网络安全的基础理论有比较全面的了解，对密码学的主要算法、技术和应用有比较全面的认识。

2.1　数据加密概述

在计算机网络中，我们需要一种措施来保护数据的安全性，防止被一些别有用心的人利用或破坏，这在客观上就需要一种强有力的安全措施来保护机密数据不被窃取或篡改。数据加密技术是为了提高信息系统及数据的安全性和保密性，防止秘密数据被外部破析所采用的主要技术手段之一。随着信息技术的发展，网络安全与信息保密日益引起人们的关注。我们除在法律和制度及管理手段上加强数据的安全管理外，还需要推动数据加密技术和物理防范技术的应用和不断发展。

2.1.1　数据加密的必要性

自从有了消息的传递就有了对消息保密的要求，因此可以说密码学的历史非常悠久。但在很长一段时间内，密码学主要用于军事、政治和外交等用途。

到了20世纪70年代，随着信息量的剧增，人们对信息的保密需求也从以往的军事、政治和外交迅速发展到民用和商用领域，从而导致了密码学理论和密码技术的快速发展。同时，计算机技术和微电子技术的发展，也为密码学理论的研究和实现提供了强有力的手段和工具。进入20世纪80年代以来，随着计算机网络和传统通信网络的广泛应用，对密码理论和技术的研究更呈快速上升的趋势。密码学在雷达、导航、遥控和遥测等领域发挥着重要作用的同时，开始渗透到通信、计算机及各种信息系统中。

举例来说，在学校的各项管理中越来越依赖于计算机网络。如人事管理系统、工资管理系统、账务管理系统、教务管理系统和科研成果管理系统等，其中的重要数据都存放在计算机中，不仅要求数据具有较高的安全性和保密性，而且要求对数据的完整性及访问方式进行科学管理。对企业来说，产品的核心技术需要保密，新产品的研发需要保密，企业的产、销、利润及市场策略等关键信息需要保密。即使对家庭用户来说，如个人隐私、家庭收入、现金的储蓄和投资等信息都需要保密。

因此，在全社会越来越依赖信息的同时，人们的信息安全意识越来越高，密码学和安全

技术越来越受到人们的关注。

2.1.2 数据加密的基本概念

密码技术通过信息的变换或编码,将机密的敏感消息变换成为难以读懂的乱码字符,以此达到两个目的:一是使不知道如何解密的窃听者不可能由其截获的乱码中得到任何有意义的信息;二是使窃听者不可能伪造任何乱码型的信息。研究密码技术的学科称为密码学,其中密码编码学主要对信息进行编码,实现信息隐蔽;而密码分析学研究分析破译密码的学问。两者相互对立,而又相互促进。

加密的目的是防止机密信息的泄露,同时还可以用于证实信息源的真实性,验证所接收到的数据的完整性。加密系统是指对信息进行编码和解码所使用的过程、算法和方法的统称。加密通常需要使用隐蔽的转换,这个转换需要使用密钥进行加密,并使用相反的过程进行解密。

通常,将加密前的原始数据或消息称为明文(plaintext),而将加密后的数据称为密文(ciphertext),在密码中使用并且只有收发双方才知道的信息称为密钥(key)。通过使用密钥将明文转换成密文的过程称为加密,其反向过程(将密文转换为原来的明文)称为解密。对明文进行加密时采用的一组规则称为加密算法。对密文解密时采用的一组规则称为解密算法。加密算法和解密算法是在一组仅有合法用户知道的密钥的控制下进行的,加密和解密过程中使用的密钥分别称为加密密钥和解密密钥。加密和解密的转换关系如图 2-1 所示。

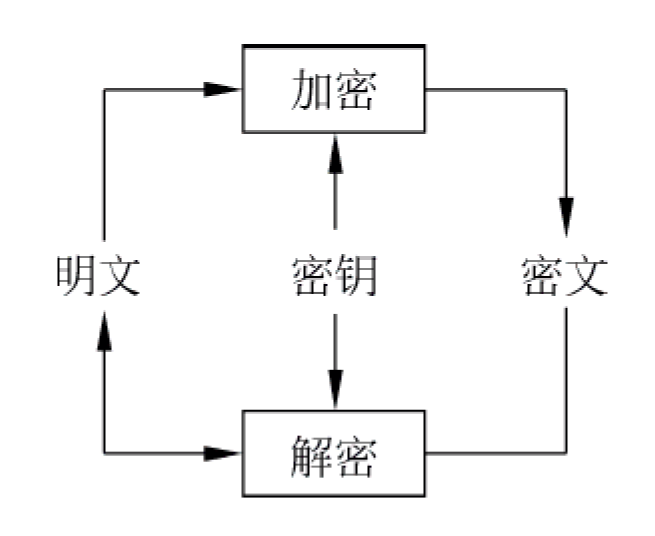


图 2-1 加密与解密的转换关系

需要说明的是,解密主要针对合法的接收者,而非法接收者在截获密文后试图从中分析出明文的过程称为"破译"。

图 2-2 是对图 2-1 加密与解密转换关系的数学表示,称为密码通信系统模型,它由以下几个部分组成。

- M:明文消息空间。
- E:密文消息空间。
- K_1 和 K_2:密钥空间。
- 加密变换:$E_{k_1}: M \rightarrow E$,其中 $k_1 \in K_1$。
- 解密变换:$D_{k_2}: E \rightarrow M$,其中 $k_2 \in K_2$。

将$(M, E, K_1, K_2, E_{k_1}, D_{k_2})$称为密码系统。例如,给定明文消息 $m \in M$,密钥 $k_1 \in K$,将明文 m 变换为密文 c 的过程为:

$$c = f(m, k_1) = E_{k_1}(m) \quad m \in M, \quad k_1 \in K_1$$

合法接收者利用其知道的解密密钥 K_2 对收到的密文进行变换,恢复出明文消息:

$$m = D_{k_2}(c) \quad m \in M, \quad k_2 \in K_2$$

如果是窃听者,则利用其选定的变换函数 h,对截获的密文 c 进行变换,得到的明文是明文空间的某个元素 m',其中:

$$m' = h(c)$$

一般情况下 $m' \neq m$,如果 $m' = m$,则窃听者已破译成功。

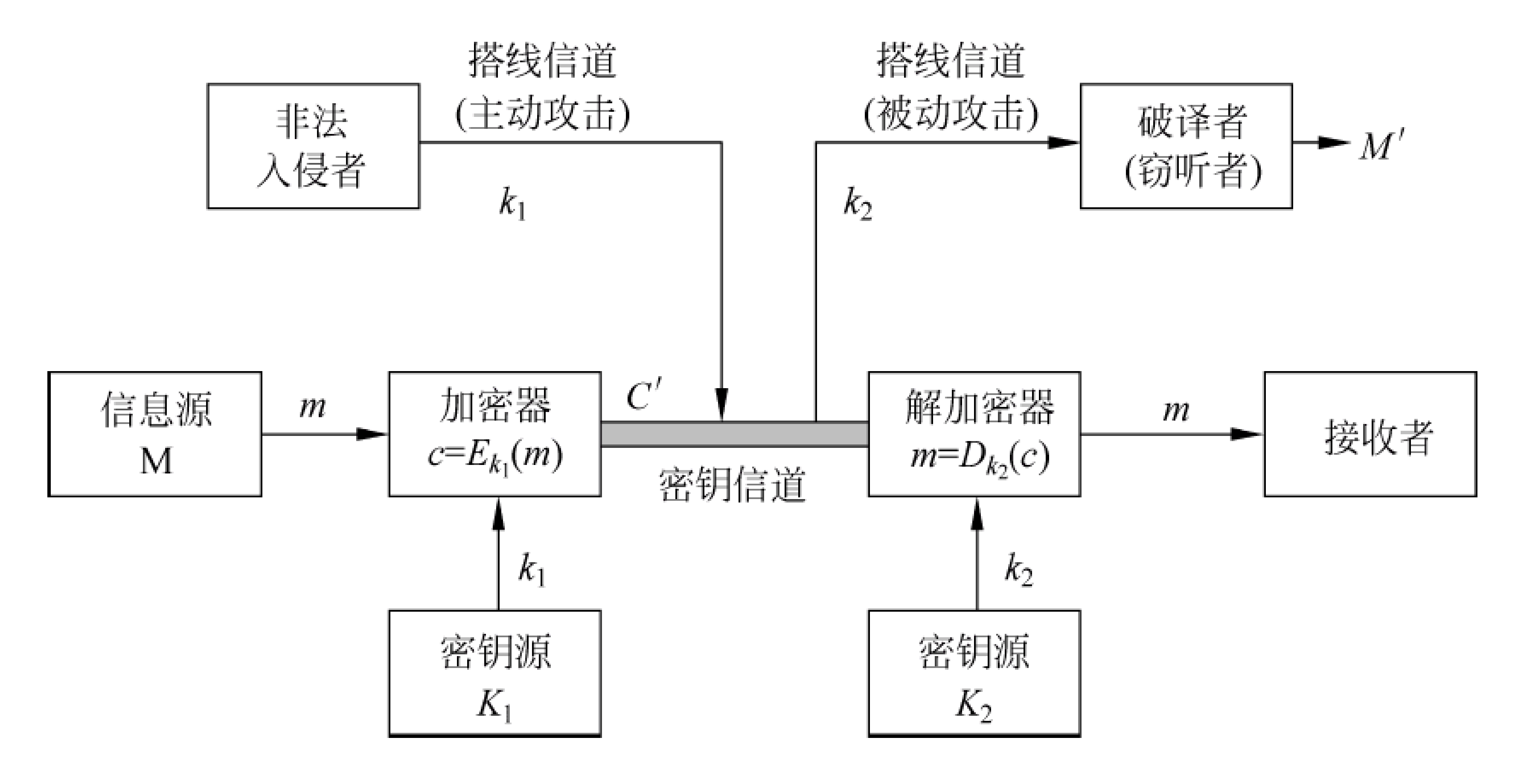


图 2-2　密码通信系统模型

2.1.3　对称加密和非对称加密

目前已经设计出的密码系统是各种各样的。如果以密钥为标准,可将密码系统分为单钥密码系统和双钥密码系统。其中,单钥密码系统又称为对称密码或私钥密码系统,双钥密码系统又称为非对称密码或公钥密码系统。相应的,采用单钥密码系统的加密方法,同一个密钥可同时用作信息的加密和解密,这种加密方法称为对称加密,也称作单密钥加密。另一种是采用双钥密码系统的加密方法,在一个过程中使用两个密钥,一个用于加密,另一个用于解密,这种加密方法称为非对称加密,也称为公钥加密,因为其中的一个密钥是公开的(另一个则需要保密)。

1. 对称加密

对称加密的缺点是密钥需要通过直接复制或网络传输的方式由发送方传给接收方,同时无论加密还是解密都使用同一个密钥,所以密钥的管理和使用很不安全。如果密钥泄露,则此密码系统便被攻破。另外,通过对称加密方式无法解决消息的确认问题,并缺乏自动检测密钥泄露的能力。对称加密的优点是加密和解密的速度快。最具有影响力的对称加密方式是 1977 年美国国家标准技术委员会(NIST,其前身为美国国家标准局 NBS)颁布的 DES 算法。

2. 非对称加密

在非对称加密中,加密密钥与解密密钥不同,此时不需要通过安全通道来传输密钥,只需要利用本地密钥发生器产生解密密钥,并以此进行解密操作。由于非对称加密的加密和解密不同,且能够公开加密密钥,仅需要保密解密密钥,所以不存在密钥管理问题。非对称加密的另一个优点是可以用于数字签名。但非对称加密的缺点是算法一般比较复杂,加密和解密的速度较慢。非对称加密是 1976 年 W. Diffie 和 M. E. Hellman 提出的一种新型密码体制,最有名的非对称加密方式是 1977 年由 Rivest、Shamir 和 Adleman 共同提出的 RSA 密码体制。

在实际应用中,一般将对称加密和非对称加密两种方式混合在一起来使用。即在加密和解密时采用对称加密方式,密钥传送则采用非对称加密方式。这样既解决了密钥管理的困难,又解决了加密和解密速度慢的问题。

2.1.4 序列密码和分组密码

根据密码算法对明文处理方式的标准不同,可以将密码系统分为序列密码和分组密码两类。

1. 序列密码

序列密码也称为流密码,其思想起源于 20 世纪 20 年代,最早的二进制序列密码系统是 Vernam 密码。Vernam 密码将明文消息转化为二进制数字序列,密钥序列也为二进制数字序列。加密是按明文序列和密钥序列逐位模 2 相加(即异或操作 XOR)进行,解密也是按密文序列和密钥序列逐位模 2 相加进行。

当 Vernam 密码中的密钥序列是完全随机的二进制序列时,就是著名的"一次一密"密码(在本章随后专门进行介绍)。一次一密密码是完全保密的,但它的密钥产生、分配和管理都不方便。随着微电子技术和数学理论的发展,基于伪随机序列的序列密码应运而生。序列密码的加密过程是先把报文、语音、图像和数据等原始明文转换成明文数据序列,然后将它同密钥序列进行逐位加密生成密文序列发送给接收者。接收者用相同的密钥序列对密文序列进行逐位解密来恢复明文序列。序列密码不存在数据扩展和错误传播,实时性好,加密和解密实现容易,因而是一种应用广泛的密码系统。

2. 分组密码

分组密码的加密方式是先将明文序列以固定长度进行分组,然后将每一组明文用相同的密码和加密函数进行运算。为了减小存储量,并提高运算速度,密钥的长度一般不大,因而加密函数的复杂性成为系统安全的关键。分组密码的优点是不需要密钥同步,具有较强的适用性,适宜作为加密标准。缺点是加密速度慢。DES 和 DEA 是典型的分组密码。

2.1.5 网络加密的实现方法

基于密码算法的数据加密技术是所有网络上的通信安全所依赖的基本技术。目前对网络数据加密主要有链路加密、节点对节点加密和端对端加密三种实现方式。

1. 链路加密

链路加密又称在线加密,它是对在两个网络节点间的某一条通信链路实施加密,是目前网络安全系统中主要采用的方式。链路加密能为网上传输的数据提供安全保证,所有消息在被传输之前进行逐位加密,在每一个节点对接收到的消息进行解密,然后使用下一个链路的密钥对消息进行加密后再进行传输。在链路加密方式中,不仅对数据报文的正文加密,而且把路由信息、校验和等控制信息全部加密。所以,当数据报文传输到某一个中间节点时,必须先被解密以获得路由信息和检验和,进行路由选择、差错检测,然后再被加密,发送给下一个节点,直到数据报文到达目的节点为止。

如图 2-3 所示,在链路加密方式下,只对通信链路中的数据加密,而不对网络节点内的数据加密。因此在中间节点上的数据报文是明文出现的,而且要求网络中的每一个中间节点都要配置安全单元(即信息加密设备)。相邻两个节点的安全单元使用相同的密钥。这种使用不是很方便,因为需要网络设施的提供者(如线路运营商)的配合,修改每一个交换节点,这种方式在广域网上显然是不太现实的。在传统的加密算法中,用于解密消息的密钥与用于加密的密钥是相同的,该密钥必须被秘密保存,并按一定规则进行变化。这样,密钥分

配在链路加密系统中就成了一个问题,因为每一个节点必须存储与其相连接的所有链路的加密密钥,这就需要对密钥进行物理传送或者建立专用网络设施。而网络节点地理分布的广阔性使得这一过程变得复杂,同时增加了密钥连续分配时的费用。链路加密方式的优点是应用系统不受加密和解密的影响,所以容易被采用。

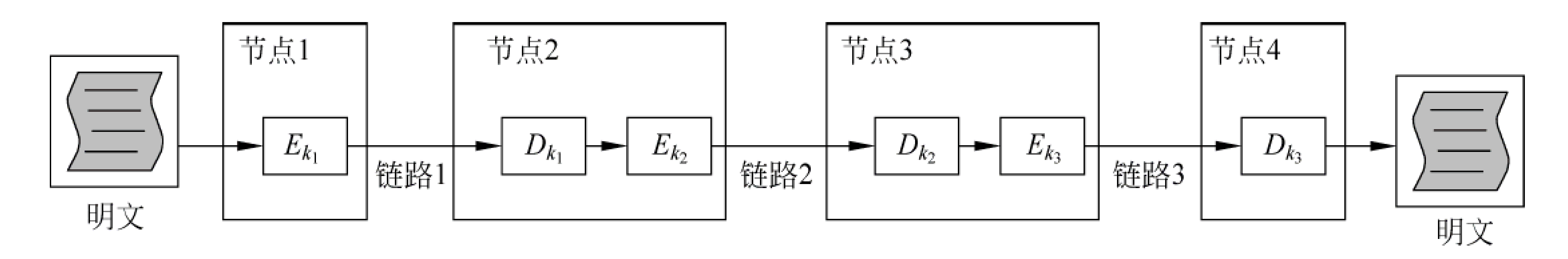


图 2-3　链路加密过程示意图

2. 节点对节点加密

节点对节点加密是为了解决在节点中的数据是明文的这一缺点,在中间节点里装有用于加密和解密的保护装置,由这个装置来完成一个密钥向另一个密钥的交换。因而,除了在保护装置里,即使在节点内也不会出现明文。

尽管节点对节点加密能给网络数据提供较高的安全性,但它在操作方式上与链路加密类似:两者均在通信链路上为传输的消息提供安全性;都在中间节点先对消息进行解密,然后进行加密。因为要对所有传输的数据进行加密,所以加密过程对用户是透明的。然而,与链路加密不同,节点对节点加密不允许消息在网络节点以明文形式存在,它先把收到的消息进行解密,然后采用另一个不同的密钥进行加密,这一过程是在节点上的一个安全模块中进行。节点对节点加密要求报头和路由信息以明文形式传输,以便中间节点能快速得到路由信息和校验和,加快消息的处理速度。

但是,节点对节点加密与链路加密方式一样存在一个共同的弱点:需要公共网络提供者的配合,修改公共网络的交换节点,增加安全单元或保护装置。

3. 端对端加密

为了解决链路加密和节点对节点加密中存在的不足,人们提出了端对端加密方式。端对端加密又称脱线加密或包加密,它允许数据在从源节点被加密后,到终点的传输过程中始终以密文形式存在。消息在到达终点之前不进行解密,只有消息到达目的节点后才被解密。因为消息在整个传输过程中均受到保护,所以即使有节点被损坏也不会使消息泄露。因此,端对端加密方式可以实现按各通信对象的要求改变加密密钥,以及按应用程序进行密钥管理等,而且采用这种方式可以解决文件加密问题。

链路加密方式是对整个链路通信采取保护措施,而端对端加密方式则是对整个网络系统采取保护措施。端对端加密系统更容易设计、实现和维护,且成本相对较低。端对端加密还避免了其他加密系统所固有的同步问题,因为每个报文段均是独立被加密的,所以一个报文段所发生的传输错误不会影响后续的报文段。此外,端对端加密方式不依赖于底层网络基础设施,不但在局域网内部可以实施,也可以在广域网上实施。端对端加密系统通常不允许对消息的目的地址进行加密,这是因为每一个消息所经过的节点都要用此地址来确定如何传输消息。因此,端对端加密方式是未来的发展趋势。

由于端对端加密方法不能掩盖被传输消息的源节点与目的节点,因此它对于防止攻击者分析通信业务是脆弱的。

2.1.6 软件加密和硬件加密

目前具体的数据加密实现方法主要有两种：软件加密和硬件加密。

1. 软件加密

软件加密一般是用户在发送信息前，先调用信息安全模块对信息进行加密处理，然后进行发送。到达接收端后，由用户用相应的解密软件进行解密处理，还原成为明文。采用软件加密方式的优点是：已有标准的安全API(信息安全应用程序模块)产品，且实现方便，兼容性好。但是采用软件加密方式有如下一些安全隐患。

(1) 密钥的管理很复杂，这也是目前安全API实现的一个难题，从目前已有的API产品来看，密钥分配协议均存在一定的缺陷。

(2) 因为加密和解密过程都是在用户的计算机内部进行，所以容易给攻击者采用程序跟踪、反编译等手段进行攻击。

(3) 软件加密的速度相对较慢。

2. 硬件加密

硬件加密是采用专门的硬件设备实现消息的加密和解密处理。随着微电子技术的发展，现在许多加密产品都是特定的硬件加密形式。这些加、解密芯片被嵌入到通信线路中，然后对所有通过的数据进行加密和解密处理。虽然软件加密在今天变得很流行，但是硬件加密仍然是商业和军事应用的主要选择。硬件加密的特点如下。

(1) 易于管理。硬件加密可以采用标准的网络管理协议(如SNMP或CMIP等)来进行管理，也可以采用统一的自定义网络管理协议进行管理，因此密钥的管理比较方便。

(2) 处理速度快。加密算法通常含有很多对明文位的复杂运算，这要求处理设备具有较强的处理能力。例如，目前常用的加密算法DES和RSA在普通用途的微处理器上的运行效率是非常低的。另外，加密通常是高强度的计算任务，微处理器显然不适合处理此类工作。如果将加密操作移植到专用芯片上，可以分担计算机微处理器的工作，使整个系统的速度加快。

(3) 安全性提高。可以对加密设备进行物理隔离，使得攻击者无法对其进行直接攻击。对运行在没有物理保护的一般主机上的每个加密算法，很可能被攻击者用各种跟踪工具攻击。硬件加密设备可以安全地封装起来，以避免此类事情的发生。

(4) 易于安装。在用于加密的两个节点之间部署加密设备非常简单，不需要修改计算机和网络的任何配置。对用户来说，加密设备是透明的，不会影响用户的使用。如果要实现软件加密，需要将加密程序写入操作系统或应用软件，实现比较复杂。

2.2 古典密码介绍

本节简要介绍几种古典密码体制。虽然这些密码现在已经很少使用，但它们对于理解和分析现代实用密码是很有意义的。

2.2.1 简单替换密码

简单替换密码是古典密码中使用最早的一种密码机制，其实现方法是将明文按字母表中当前的位置向后移动 n 位，便得到加密后的密文，这里的 n 就是密钥。例如，当 $n=3$(即

以 $n=3$ 为密钥）时，字符表的替换如下（为便于表述，约定在明文中使用小写字母，而在密文中使用大写字母）。

明文：a b c d e f g h i j k l m n o p q r s t u v w x y z

密文：D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

在简单替换密码体制中，加密时，将明文的每一个字母根据字母表中的位置向后移动 n 位得到密码文。解密时，将密文中的每一个字母根据字母表中的位置向前移动 n 位便得到明文。使用简单替换密码时，明文 attack 将被变换为 DWWDFN。

当 $n=3$ 时的密码体制由于被恺撒（Caesar）成功使用，所以也称为恺撒密码。

在简单替换密码中，所有可能的密码 n 的取值为 $n\in\{1,2,3,\cdots25\}$。当 $n=0$ 和 $n=26$ 时明文和密文相同。

当攻击者得到一个密文，并且知道该密码是采用简单替换密码进行加密处理而来时，最多可经过 25 种尝试，就可以得到明文。所以简单替换密码的密钥空间是很有限的。

由于简单替换密码的不可靠性，所以后来人们对它进行了改进，让明文中的每一个符号（包括字母、数字及特殊符号等）都映射到另一个指定的符号上，如下所示（以字母映射为例）。

明文：a b c d e f g h i j k l m n o p q r s t u v w x y z

密文：Q W E R T Y U I O P A S D F G H J K L Z X C V B N M

这种“符号对符号”进行替换的通用系统称为“单字母表替换”，其密钥是对应于整个字母表的 26 个字母串。明文 attack 将被变换为 QZZQEA。

与简单替换密码相比，这种“符号对符号”的密码是非常安全的，因为密码分析者要想试遍所有的密钥不是一件容易的事情。以 26 个字母之间的映射为例，密钥的可能性总共有 $26!\approx4\times10^{26}$ 种。

2.2.2 双重置换密码

使用双重转换密码进行加密时，首先将明文写成给定大小的矩阵形式，然后根据给定的置换规则对行和列分别进行置换。例如，对明文 attackattomorrow 写成 4×4 的矩阵形式：

$$\begin{bmatrix} a & t & t & a \\ c & k & a & t \\ t & o & m & o \\ r & r & o & w \end{bmatrix}$$

然后，按照(1,2,3,4)→(2,3,4,1)的规则进行行置换，然后再按照(1,2,3,4)→(3,4,2,1)的规则进行列置换。操作如下：

$$\begin{bmatrix} a & t & t & a \\ c & k & a & t \\ t & o & m & o \\ r & r & o & w \end{bmatrix} \to \begin{bmatrix} c & k & a & t \\ t & o & m & o \\ r & r & o & w \\ a & t & t & a \end{bmatrix} \to \begin{bmatrix} a & t & k & c \\ m & o & o & t \\ o & w & r & r \\ t & a & t & a \end{bmatrix}$$

从而得到的密文为 ATKCMOOTOWRRTATA。

在双重置换密码体制中，密钥由矩阵的大小及行、列置换规则组成。接收者如果知道密钥，就可以通过加密过程使用的矩阵大小及行、列的置换规则来进行逆向操作，从而恢复得

到明文。例如,对于前面得到的密文,可以先写成 4×4 的矩阵形式,然后将列进行(3,4,2,1)→(1,2,3,4)的置换,再将行进行(2,3,4,1)→(1,2,3,4)的置换。操作如下:

$$\begin{bmatrix} A & T & K & C \\ M & O & O & T \\ O & W & R & R \\ T & A & T & A \end{bmatrix} \rightarrow \begin{bmatrix} C & K & A & T \\ T & O & M & O \\ R & R & O & W \\ A & T & T & A \end{bmatrix} \rightarrow \begin{bmatrix} A & T & T & A \\ C & K & A & T \\ T & O & M & O \\ R & R & O & W \end{bmatrix}$$

于是得到明文 attackatwomorrow。

与简单替换密码相比,双重置换密码并不改变消息中的字符,只是对字符进行重新组合,这样可以抵抗基于明文中包含的统计信息的攻击。虽然双重置换密码目前已很少使用,但其明文与密文信息之间的转换思想在现代密码学中被广泛采用。

2.2.3 "一次一密"密码

最著名的序列密码是"一次一密"密码,也称为"一次一密乱码本加密机制"。其中,一次一密乱码本是一个大的不重复的随机密钥字符集,这个密钥字符集被写在几张纸上,并粘合成一个本子,该本子称为乱码本。每个密钥仅对一个消息使用一次。发送方用乱码本中的密钥对所发送的消息加密,然后销毁乱码本中用过的一页或用过的磁带部分。接收方有一个同样的乱码本,并依次使用乱码本上的每一个密钥去解密密文的每个字符。接收方在解密消息后销毁乱码本中用过的一页或用过的磁带部分。新的消息则用乱码本的新密钥进行加密和解密。"一次一密"密码是一种理想的加密方案,理论上讲,实现了"一次一密"密钥管理的密码是不可破译的。

为了描述方便,假设明文全部使用 ASCII 码中的字符。首先需要将明文(本例假设为 attack)转换成为 7 位的 ASCII 码。attack 对应的 ASCII 码如下。

明文:　　a　　t　　t　　a　　c　　k

ASCII 码:01100001 01110100 01110100 01100001 01100011 01101011

使用"一次一密"密码体制加密时,需要与明文长度相同的随机二进制字符串作为密钥。密钥与明文进行一对一的逐位模 2 相加运行得到密文。假设发送者使用的加密密钥为:

11000101 10011101 01011000 00111011 11001011 00011010

那么加密过程如下。

　　　a　　t　　t　　a　　c　　k

明文:01100001 01110100 01110100 01100001 01100011 01101011

密钥:11000101 10011101 01011000 00111011 11001011 00011010

密文:10100100 11101001 00101100 01011010 10101000 01110001

　　　$　　i　　,　　Z　　(　　q

通过以上转换,得到的密文字符为 $i,Z(q。当接收者收到该密文后,使用相同的密钥进行解密操作。因为根据模 2 相加运行的法则,将二进制的 x 和 y 的模 2 相加可以记作 $x \oplus y$,其中 $x \oplus y \oplus y = x$,所以解密过程是将密文与同样的密钥进行模 2 相加运算。具体操作如下。

$　　　i　　　,　　　Z　　　(　　　q

密文：10100100 11101001 00101100 01011010 10101000 01110001

密钥：11000101 10011101 01011000 00111011 11001011 00011010

明文：01100001 01110100 01110100 01100001 01100011 01101011

a　　　t　　　t　　　a　　　c　　　k

通过以上操作，原始的明文就恢复了出来。

通过以上的加密和解密过程可以发现，如果密钥是随机产生的，"一次一密"密码是非常安全的。当然，该安全性是建立在密码被正确使用的前提下：一是密钥是随机产生的；二是密钥只使用一次；三是只有发送者和接收者知道该密钥。

2.3　对称加密——流密码

流密码(即序列密码)是一种类似于"一次一密"密码体制，因为在加密过程中是将密钥流(密钥的二进制位)与等长的明文的二进制位进行模 2 运算，在解密过程中是将密钥流与密文进行逐位模 2 运算，所以流密码是一种对称加密方式。

2.3.1　流密码的工作原理

在现代计算机网络中，由于报文、数据和图像等消息都可以通过某一编码技术转化为二进制数字序列，因而可假定流密码中的明文空间 M 是由所有可能的二进制数字序列组成的集合。设 K 为密钥空间，由于流密码应使用尽可能长的密钥，而太长的密钥在存储、分配等方面都有一定的困难，于是研究人员采用一个短的密钥 $k \in K$ 来控制某种算法 A 产生出长的密钥序列，供加密和解密使用。而短密钥 k 的存储和分配在实现方式上都比较容易。根据密码学的约定，算法 A 是公开的，而密钥 k 是保密的。

流密码系统的工作过程如图 2-4 所示。即对于每一个短密钥 $k \in K$，由算法 A 确定一个二进制序列 $A(k)=k_1,k_2\cdots,k_n$，当明文为 $m \in M, m=m_1,m_2,\cdots,m_n$ 时，使用密钥 k 的加密过程为：对于 $i=1,2,\cdots,n$，计算 $c_i=m_i \oplus k_i$，密文为 $c=E(m,k)=c_1,c_2,\cdots,c_n$，其中$\oplus$表示模 2 运算。对密文 c 的解密过程为：对于 $i=1,2,\cdots,n$，计算 $m_i=c_i \oplus k_i$，由此恢复明文 m。通常称密钥 k 为种子密钥或子密钥，由 k 通过算法 A 产生的序列 $A(k)=k_1,k_2,\cdots,k_n$ 称为密钥序列。

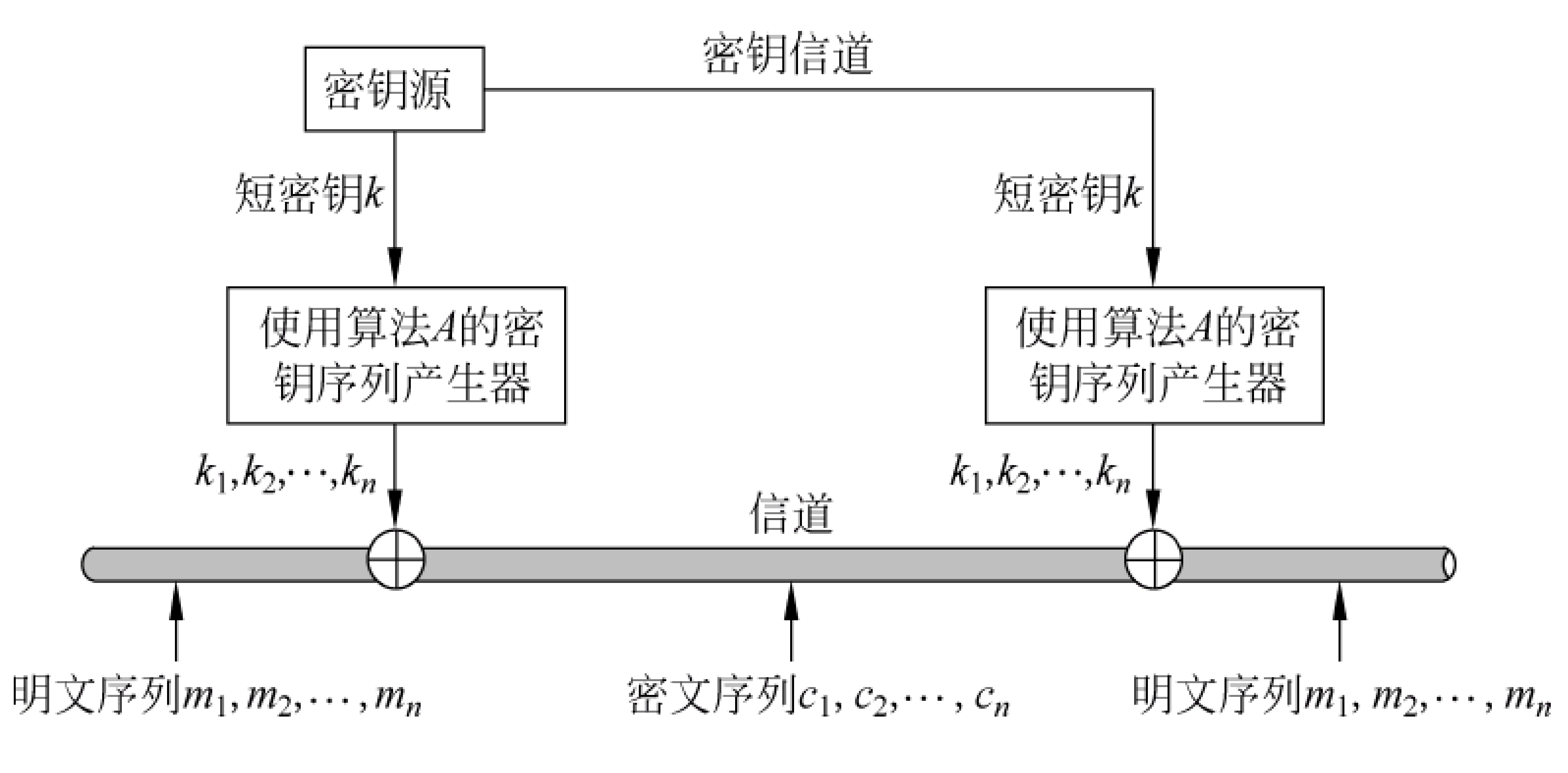


图 2-4　流密码系统的工作过程

由此可以看出，流密码的安全性主要依赖于密钥序列 $A(k)=k_1,k_2,\cdots,k_n$，当 $k_1,k_2,\cdots,k_n$ 是离散的、不便于记忆的二进制密钥源产生的随机序列时，该系统就是“一次一密”密码。但通常 $A(k)$ 是一个由 k 通过确定算法 A 产生的伪随机序列，因而此时该系统就不再是完全安全的。

到目前为止，流密钥序列的产生大多数是基于硬件的移位寄存器来实现的，因为移位寄存器结构简单，运行速度快。

2.3.2　A5/1

A5/1 是一个可以在硬件上高效实现的流密码算法，是在欧洲数字蜂窝移动电话系统(Global System for Mobill Communications，GSM)中采用的流密码加密标准。

1. A5/1 的数学描述

A5/1 使用标号为 X、Y 和 Z 的三个线性移位寄存器。其中，寄存器 X 占有 19 位的存储空间，编号为$(x_0,x_1,\cdots,x_{18})$；寄存器 Y 占有 22 位的存储空间，编号为$(y_0,y_1,\cdots,y_{21})$；寄存器 Z 占有 23 位的存储空间，编号为$(z_0,z_1,\cdots,z_{22})$。这三个寄存器共占有 64 位的存储空间。

根据流密码的要求，密钥同样也需要占有 64 位的空间，用于初始化 X、Y 和 Z 这三个寄存器。当用密钥填充完三个寄存器(即初始化操作)后，就做好了产生密钥流的准备。

在描述密钥流的产生之前，先介绍 X、Y 和 Z 这三个寄存器的操作方式。

X 寄存器的操作过程为：

$$t = x_{13} \oplus x_{16} \oplus x_{17} \oplus x_{18}$$
$$x_i = x_{i-1},\quad i = 18,17,16,\cdots,1$$
$$x_0 = t$$

Y 寄存器的操作过程为：

$$t = y_{20} \oplus y_{21}$$
$$y_i = y_{i-1},\quad i = 21,20,19,\cdots,1$$
$$y_0 = t$$

Z 寄存器的操作过程为：

$$t = z_7 \oplus z_{20} \oplus z_{21} \oplus z_{22}$$
$$z_i = z_{i-1},\quad i = 22,21,20,\cdots,1$$
$$z_0 = t$$

在计算密钥流时，给定三个位 x、y 和 z，定义一个函数 $\mathrm{maj}(x,y,z)$，该函数确定了这样一个法则：如果 x、y、z 中的多数为 0，则函数返回值为 0，否则返回值为 1。这样，A5/1 每步操作将产生 1 位的密钥流。这种计算速度虽然看上去很慢，但因为 A5/1 是专门根据硬件实现来设计的，所以产生密钥流的速度还是很快的。

2. A5/1 的硬件实现

A5/1 是用硬件来实现的。硬件实现必须考虑其时钟周期，A5/1 的时钟周期的计算为：

$$m = \mathrm{maj}(x_8,y_{10},z_{10})$$

这样，X、Y 和 Z 这三个寄存器将根据以下的规则进行操作：如果 $x_8=m$，则进行 X 操

作；如果 $y_{10}=m$，则进行 Y 操作；如果 $z_{10}=m$，则进行 Z 操作。最后密码流位按照以下方式产生：

$$s = x_{18} \oplus y_{21} \oplus z_{22}$$

加密时，密钥流 s 与明文进行模 2 运算。解密时，使用密钥流 s 与密文进行模 2 运算。

图 2-5 所示的是 A5/1 密钥流生成器的结构示意图。其中，密钥流中位的产生速度与该硬件系统的时钟频率相当。

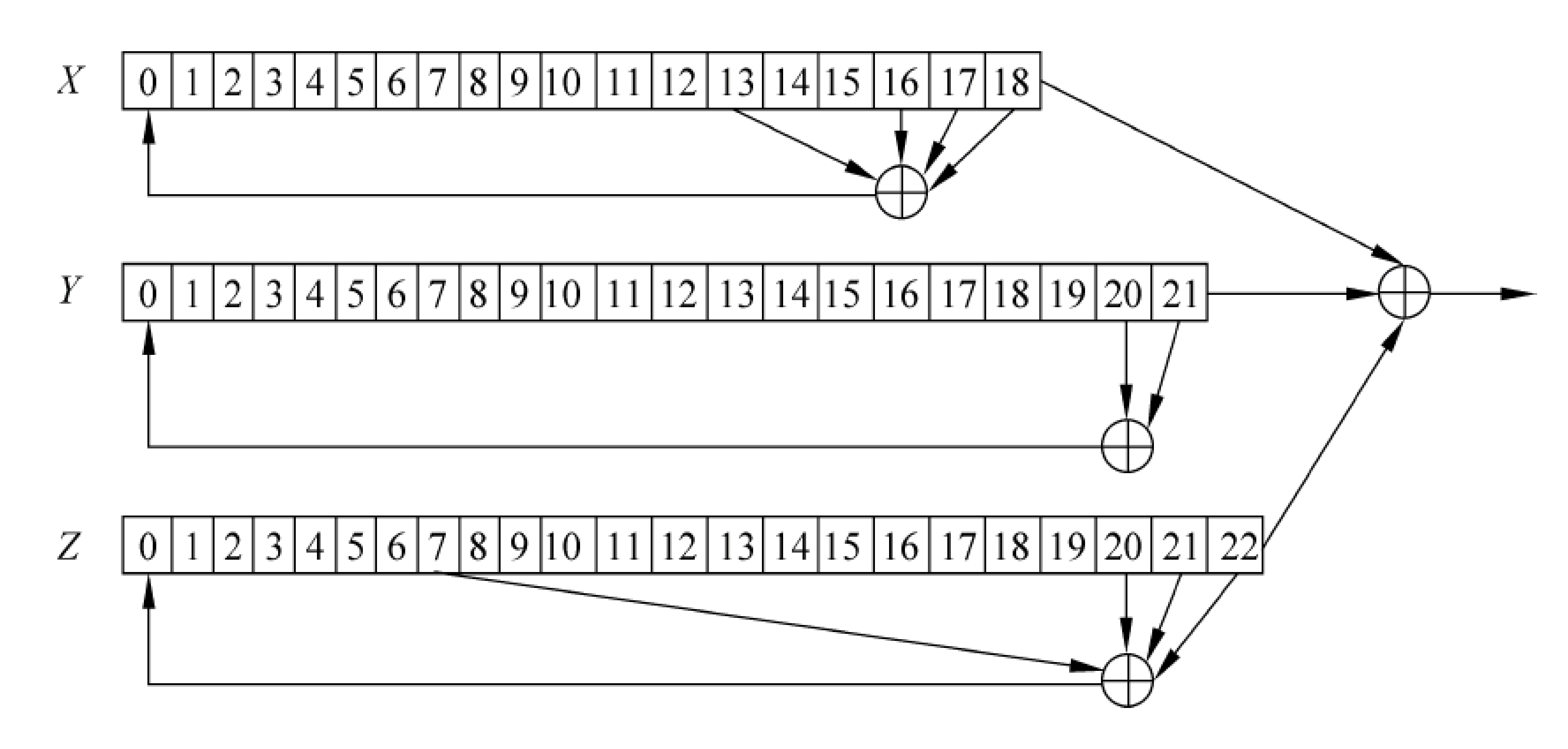


图 2-5　A5/1 密钥流生成器的工作过程

需要说明的是，基于移位寄存器及硬件实现的 A5/1 算法是早期流密码的应用代表，它曾经是对称密码的主流。但是随着近年来分组密码的广泛应用，A5/1 在许多应用中已经被分组密码所替代。另外，基于软件实现的流密码 RC4 目前的应用较为广泛。有关 RC4 的内容有兴趣的读者可以参阅相关的技术文献。

2.4　对称加密——分组密码

流密码和分组密码都属于对称密钥算法，流密码的基本思想是利用密钥产生一个密钥流，并通过相应的规则对明文串进行加密和解密处理。而分组密码是将明文分为固定长度的分组，然后通过若干轮(round)函数的迭代操作来产生密文。函数由于在每一轮的操作中都使用，所以称为轮函数，其本轮的输入是上一轮的输出加上密钥。

2.4.1　Feistel 密码结构

Feistel 密码结构是以密码学的先驱美国 Horst Feistel 的名字来命名的，这是密码设计的一个结构，而非一个具体的密码产品(类似于 TCP/IP 参考模型)。现在正在使用的几乎所有重要的对称分组密码都使用 Feistel 结构。

如图 2-6 所示，在 Feistel 密码结构中，大小为 $2w$ 位的明文 P 被平均分成左右两部分(各 $1w$ 位，分别用 L_0 和 R_0 表示)：

$$P = (L_0, R_0)$$

第 1 轮(round)加密时分别输入明文 L_0 和 R_0 及子密钥 k_1。输出也分为左右两部分，其中左半部分 L_1 直接用原来的右半部分 R_0 来替换，而右半部分 R_1 的获得要经过两步操作：第一步是以子密钥 k_1 为参数对右边半部分 R_0 用轮函数 F 进行计算；第二步是利用第

一步的函数输出值(密钥)与左半部分 L_0 进行模 2 运算,以上两步操作得到的值即 L_1。

采用相同的方法,每一轮 i 以前一轮得到的 L_{i-1} 和 R_{i-1} 为输入,另外的输入还有从总的密钥 k 生成的子密钥 k_i。对数据的左半部分进行替换操作,替换的方法是对数据右半部分应用轮函数 F,然后用这个函数的输出和数据的左半部分进行模 2 运算。之后,算法做一个置换操作,把数据的左右两个部分进行互换。以上加密操作的数学描述如下:

$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \oplus F(R_{i-1}, k_i)$$

在以上操作中,其中每一轮操作中的子密钥 k_i 是由密钥 k 通过密钥扩展算法产生的,子密钥在每一轮操作中的结构一样,但内容不同。另外,轮函数在每一轮操作中有着相同的结构,但是以各轮的子密钥 k_i 为参数进行区分。最后,密文 C 是最后一轮的输出:

$$C = (L_{n+1}, R_{n+1})$$

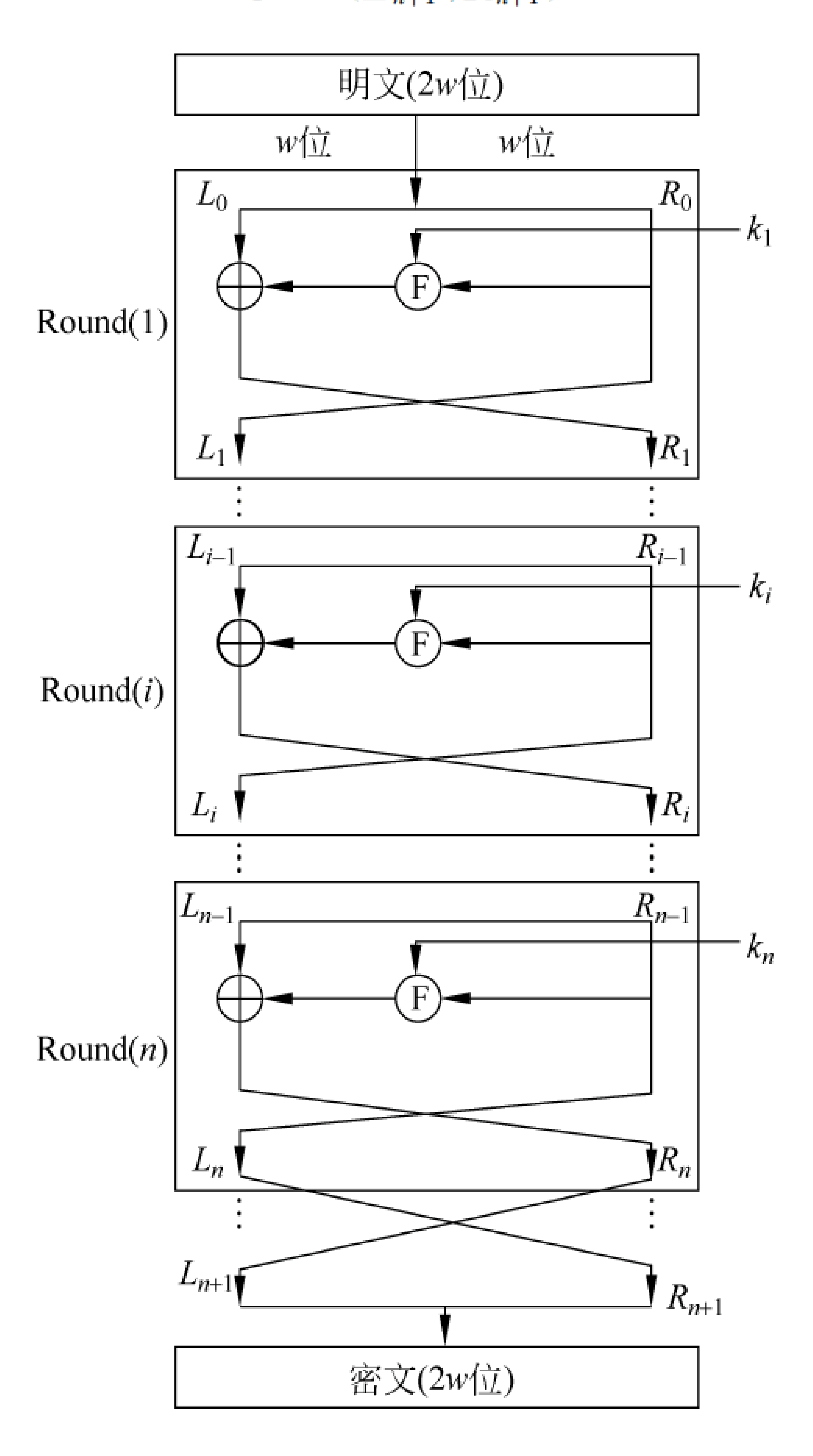


图 2-6　Feistel 网络结构

Feistel 密钥的具体实现依赖于以下的参数和设计特点。

(1) 分组大小。在其他条件相同的情况下,分组越大意味着安全性越高,但加密和解密的速度也就越慢。64 位的分组大小是一个较为合理的选择。目前在分组密码设计中几乎都使用 64 位的分组大小。

(2) 密钥大小。密钥长度越长则安全性越高,但加密和解密的速度也就越慢。64 位或者更小的密钥长度目前已被认为不安全,所以多使用 128 位的密钥长度。

(3) 循环次数。Fetstel 密码的特点是一个循环不能保证足够的安全性，而循环越多则安全性越高。目前通常使用 16 次循环。

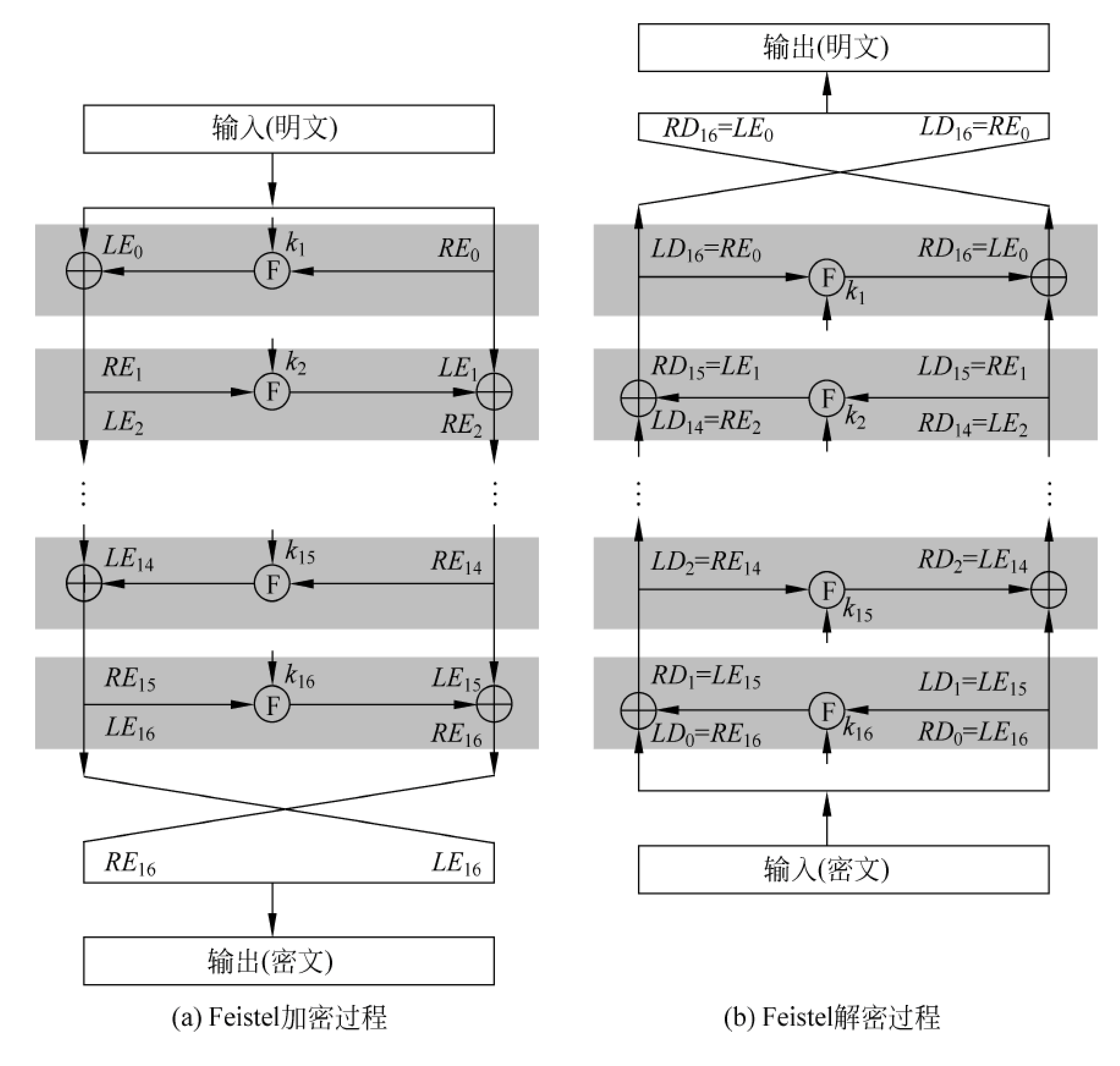
(4) 轮(round)函数。复杂性越高，则抗击密码分析的能力就越强。从实现过程来看，Feistel 结构的所有安全问题几乎都集中在轮函数的设计上。

Feistel 加密和解密的详细过程如图 2-7(a)和图 2-7(b)所示。对比 Feistel 的加密和解密过程可以发现，无论使用何种特殊的轮函数 F，都能够很容易地进行解密操作。对加密的数学描述求解 R_{i-1} 和 L_{i-1}，就可以将整个加密过程还原，得到加密之前的明文。解密规则的数学描述如下：

$$R_{i-1} = L_i$$

$$L_{i-1} = R_i \oplus F(R_{i-1}, k_i)$$

最终的结果就是原始的明文 $P=(L_0, R_0)$。



(a) Feistel加密过程　　(b) Feistel解密过程

图 2-7　Feistel 的加密和解密过程

2.4.2　数据加密标准

数据加密标准(Data Encryption Standard，DES)是由 IBM 公司在 1971 年设计的一个加密算法。1977 年由美国国家标准局(现美国国家标准技术委员会)作为第 46 号联邦信息处理标准而采用的一种数据加密标准。之后，DES 成为金融界及其他非军事行业应用最为广泛的对称加密标准。DES 是分组密码的典型代表，也是第一个被公布出来的标准算法。DES 的算法完全公开，在密码学史上开创了先河。DES 是迄今为止世界上应用最为广泛的一种分

组密码算法。虽然美国政府已经用新的数据加密标准 AES 取代了 DES,但 DES 在现代分组密码理论的发展和应用中起到了决定性作用,DES 的理论和设计思想仍有重要的参考价值。

1. DES 的算法描述

DES 是一个完全遵循 Feistel 密码结构的分组密码算法。DES 将明文以 64 位为单位分组进行加密,在一次加密过程中以 64 位为一组的明文从算法的一端输入,同时在另一端输出 64 位的密文。DES 中密钥的长度通常应为 64 位,但其中后面的 8 位作为奇偶校验使用,所以实际使用的只有 56 位。

如图 2-8 所示,DES 的基本加密过程总共有 19 个步骤。其中,第 1 步是一个与密钥无关的置换操作,它直接将 64 位的明文分为左右两部分,每一部分为 32 位。最后一步(即第 19 步)正好是对第 1 步中置换的逆操作。而第 18 步是交换左 32 位和右 32 位。其他 16 步的功能完全相同,但使用了原始密钥的不同子密钥 k_i 作为轮函数 F 的参数。

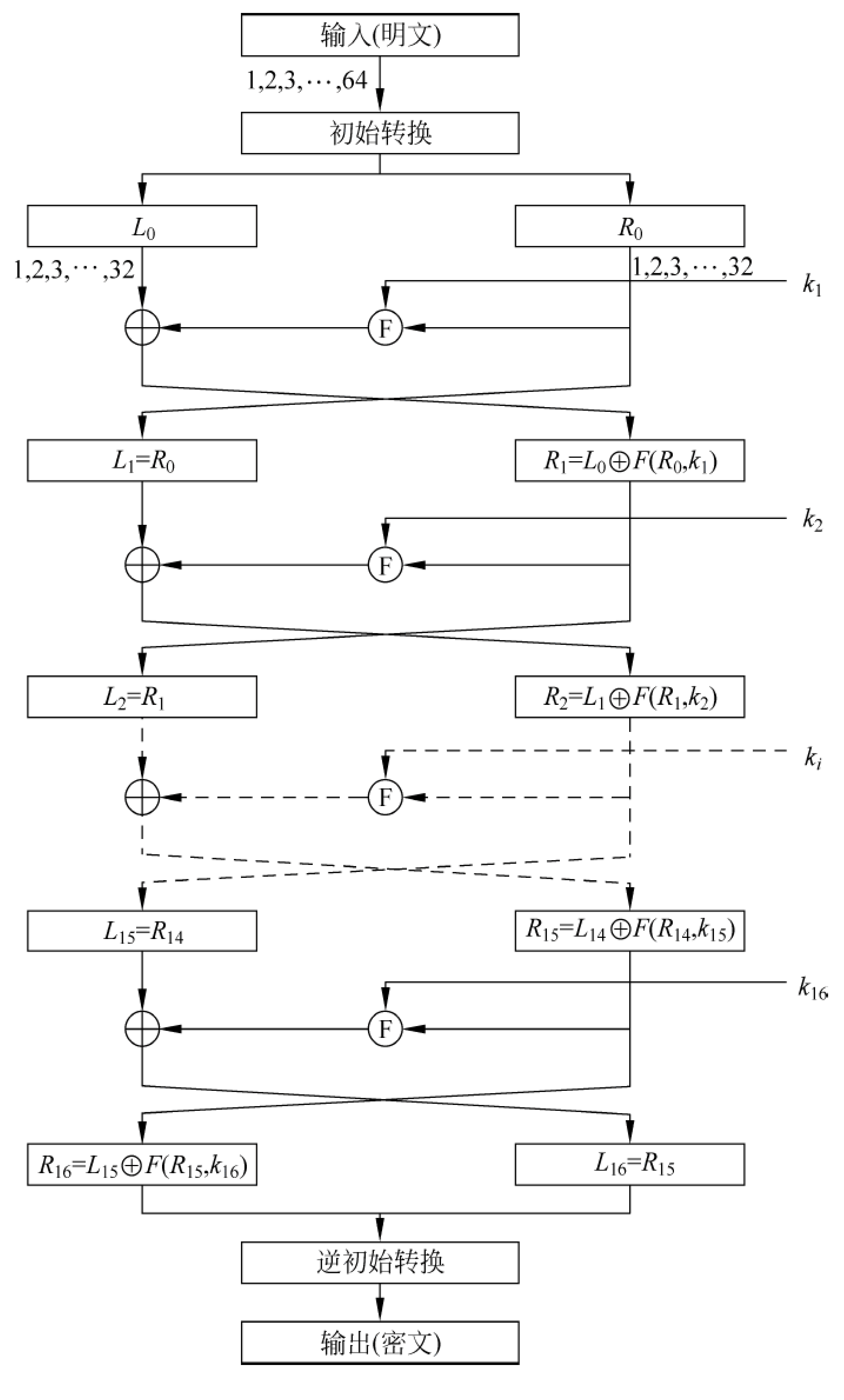


图 2-8　DES 算法示意图

DES 算法的设计允许使用同样的密钥来完成解密过程，而且解密是加密的逆过程。这正是任何一个对称密钥算法必须满足的一个条件。

下面是对 DES 的总结。

- 是使用 16 轮操作的 Feistel 结构密码。
- 分组长度为 64 位。
- 使用 56 位的密钥。
- 每一轮使用 48 位的子密钥，每一个子密钥都是由 56 位的密钥的子集构成。

2. DES 中每一轮操作的过程

图 2-9 是对图 2-6 中 16 轮 Feistel 结构密码操作中一轮的示意图。下面结合图 2-9，对图 2-8 中每一轮操作进行介绍。因为 DES 算法中每一组明文的长度为 64 位，所以根据 Feistel 结构密码的规则，将其分为左右两部分，每一部分为 32 位。与所有 Feistel 结构密码一样，每一轮的处理都遵循以下的数学描述：

$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \oplus F(R_{i-1}, k_i)$$

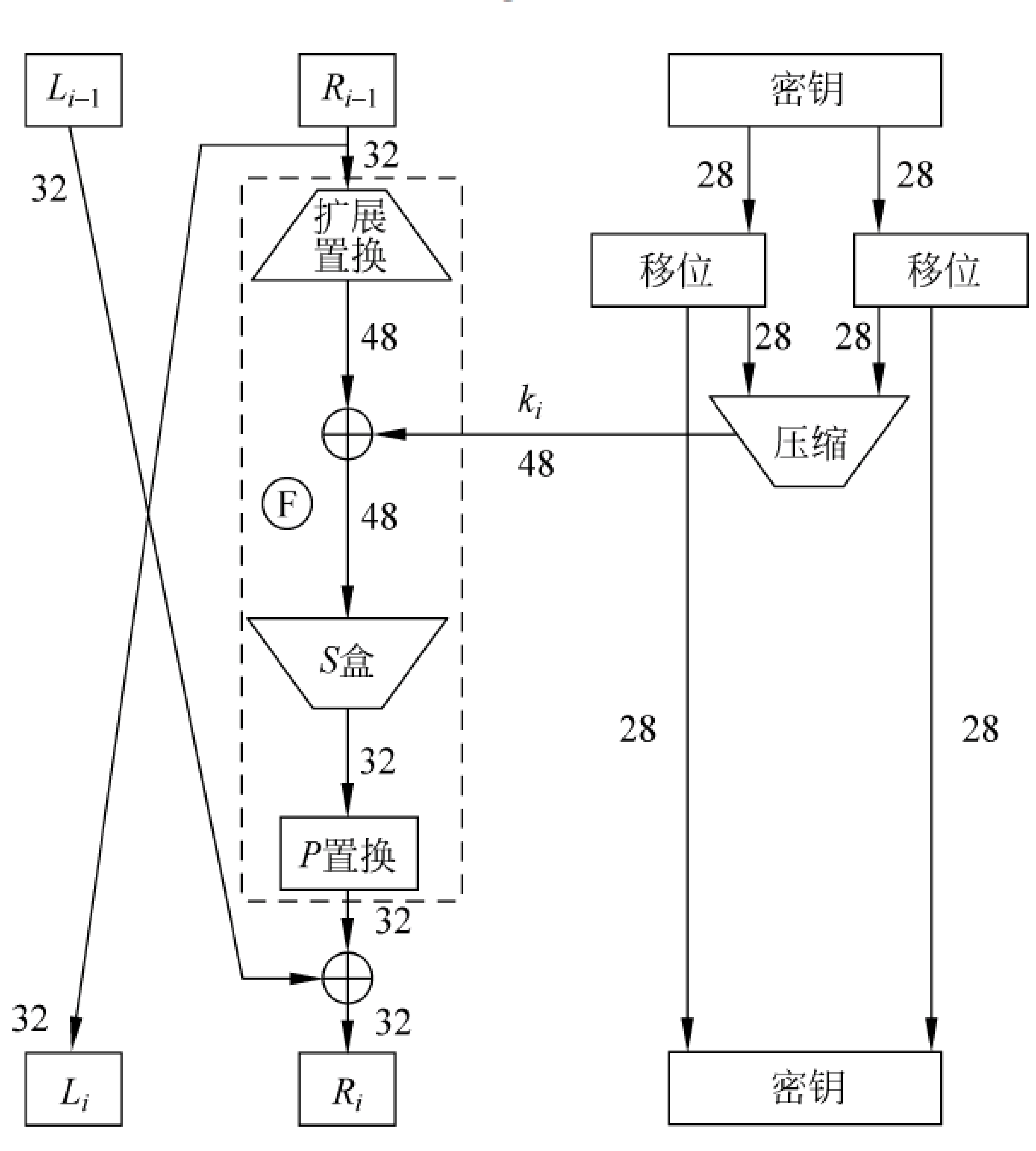


图 2-9　DES 中每一轮操作的示意图

其中轮函数 F 进行了扩展置换、子密钥相加、S 盒和 P 置换的组合操作。其中，“扩展置换”将 32 位的输入扩展为 48 位，其结果再与 48 位子密钥按位进行模 2 运算。然后“S 盒”将这 48 位压缩为 32 位，随后对“S 盒”的输出进行“P 置换”。“P 置换”的输出再与原来的左半部分(L_{i-1})按位进行模 2 运算，最终得到新的右半部分(R_i)。

图 2-9 的右半部分给出了 56 位密钥的使用方式。算法开始之前，先在 56 位的密码上执行一个 56 位的置换操作(通过置换函数)。在每一轮操作之前，密钥被分为两部分，每一部分为 28 位，然后分别进行按位的“移位”操作(具体为左移)，移动的位数取决于当前的轮操作号(具体在 0～16 之间)。移位操作后，再执行另一个 56 位的“压缩”处理，即生成 48 位

的子密钥 k_i。在每一次循环中，置换函数是相同的，但由于密钥的位进行了移位，所以每一次产生的子密钥并不相同。

3. DES 中的 S 盒

“S 盒”是 DES 算法中的核心。正是由于 S 盒的重要性，所以相关技术细节一直未被公开。这也是有人怀疑 DES 算法留有安全后门的一个原因，不过 S 盒确实增加了 DES 算法抵抗密码攻击的能力。

S 盒在轮函数 F 中的作用如图 2-10 所示。一次替换由一组共 8 个 S 盒组成。其中每一个 S 盒都接收 6 位的输入，产生 4 位的输出。这样，48 位的输入最后得到 32 位的输出。

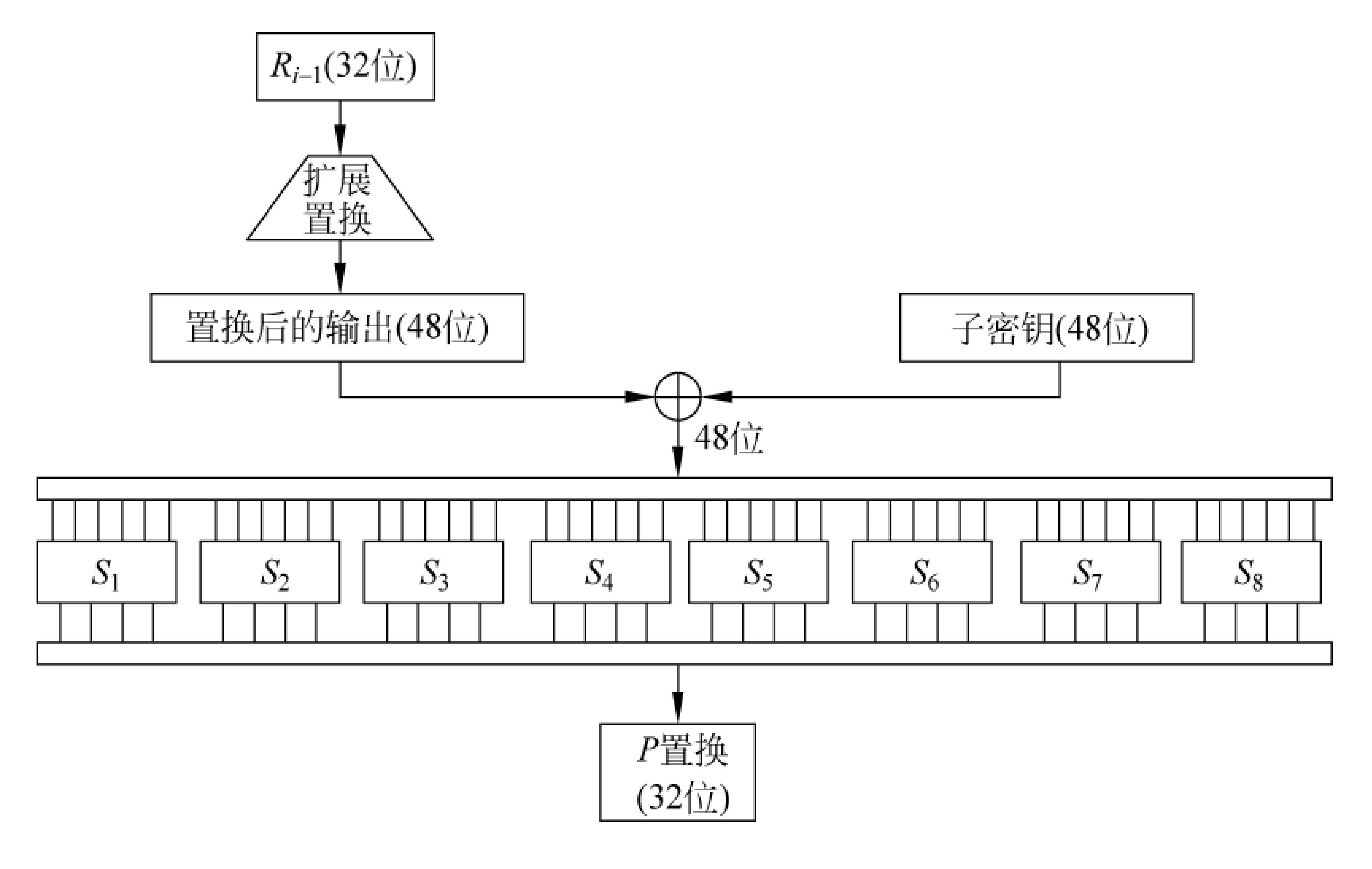


图 2-10　S 盒的替换操作

这 8 个 S 盒是不同的。每一个 S 盒是一个 4 行、16 列的矩阵，其中盒中 6 位的输入确定了其对应的输出值。盒子 S_i 的输入位以一种非常特殊的方式来确定盒中的项。假设将盒中的 6 位输入分别标记为 $b_1b_2b_3b_4b_5b_6$，其中由 b_1 和 b_6 组合成一个 2 位的数(其十进制数为 0～3)，用以确定矩阵中的行。由 $b_2b_3b_4b_5$ 组合一个 4 位的数(其十进制数为 0～15)，用以确定矩阵中的列。由以上行和列所确定的矩阵中的单元号码，将其十进制数转换为一个 4 位的二进制数后就产生了输出值。具体对应关系如图 2-11 所示。例如，其中一个盒子 S_1 的输入值为 011011，因为行的组合为 01(十进制数为 1)，所以对应矩阵中的第 1 行。因为列的组合为 1101(十进制数为 13)，即对应矩阵中的第 13 列。根据图 2-11 所示，矩阵中第 1 行第 13 列对应的是数字 5。所以，S_1 盒的输出值则为 1001。

b_1b_6	$b_2b_3b_4b_5$															
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

图 2-11　S 盒的置换结构

有关 P 置换、S 盒等内容的详细介绍读者可参阅相关的文献说明。

4. DES 算法的特点

DES 算法综合应用了置换、替换和移位等多种密码技术。在算法结构上采用了 Feistel 密码结构,结构紧凑,便于实现。在一次加密过程中,DES 使用了初始置换和逆初始置换各 1 次,置换操作 16 次,这样做的目的是将数据彻底打乱重排。S 盒是 DES 保密性的关键,它将 6 位的输入映射为 4 位的输出,是一个非线性变换(其本质是数据压缩),具有较高的保密性。

DES 算法也存在一些问题:一是 56 位的密钥长度太短,影响了 DES 的保密性;二是在 16 次迭代加密过程中,使用的 16 个子密钥可能存在弱密钥或半弱密钥现象。由于 DES 中子密钥产生过程的设计不当,在理论上有可能产生 16 个完全相同子密钥的弱密钥现象,也有可能产生 16 个子密钥中部分子密钥相同的半弱密钥现象。但是,由于弱密钥和半弱密钥的数量与子密钥的总数相比仍然是微不足道,因此在实际应用中并不会对 DES 的保密性造成较大的威胁。

2.4.3 三重数据加密标准

1979 年,在 DES 的使用过程中 IBM 已经意识到 DES 的密钥长度太短,于是设计了一种能够有效增加加密长度的算法,即三重 DES(Triple DES,三重数据加密标准)的加密标准,三重 DES 常写作 3DES。

3DES 使用两个密钥,并执行三次 DES 算法。使用两个密钥的原因是考虑到密钥长度对系统的开销,两个 DES 密钥加起来的长度为 112 位,这对于商业应用已经足够了。如果使用三个密钥其长度将会达到 168 位,对系统的要求将会提高。3DES 加密和解密过程分别如图 2-12(a)和图 2-12(b)所示,加密时为"加密→解密→加密"(即 EDE),即第一步按照常规的方式使用密钥 K_1 对明文执行 DES 加密,第二步利用密钥 K_2 对第一步中的加密结果进行解密,第三步使用密钥 K_1 对第二步的结果进行 DES 加密。令 P 为明文分组,K 为密钥,C 为相应的密文分组,三重 DES 的数学描述为:

$$C = E(D(E(P,K_1),K_2),K_1)$$

而不是:

$$C = E(E(E(P,K_1),K_2),K_3)$$

三重 DES 的解密过程为"解密→加密→解密"(即 DED),数学描述为:

$$P = D(E(D(C,K_1),K_2),K_1)$$

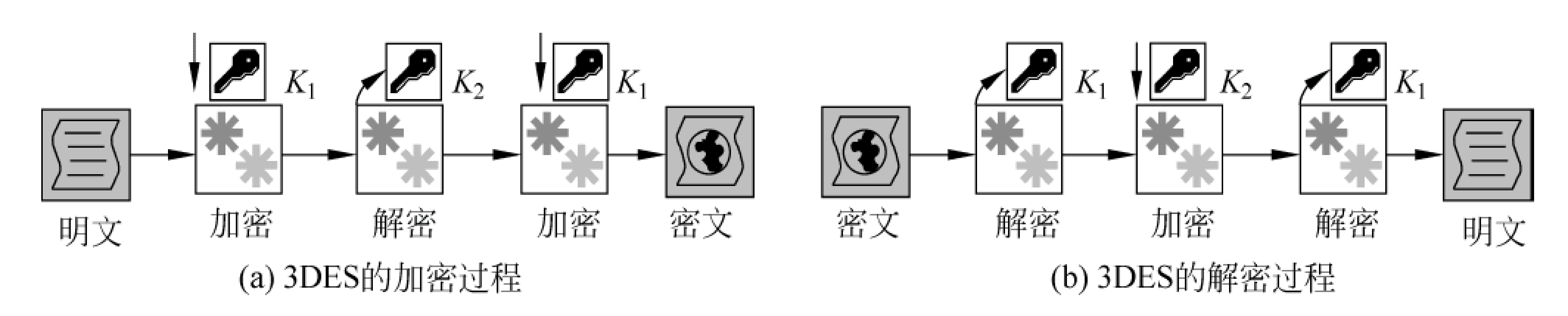


图 2-12 3DES 的加密和解密过程

通过以上介绍,读者对 3DES 的加密过程可能会产生这样的疑问:为什么使用"加密→解密→加密",而不使用"加密→加密→加密"(即 EEE)呢?这是因为采用 EDE 的目的是为了与已经被广泛使用的 DES(也称为"单密钥 DES")系统保持兼容性。由于 DES 的加密和

解密都是 64 位整数集之间的映射关系，使用 EDE 方式的 3DES 系统就可以与使用单密钥 DES 的系统进行通信，在实现过程中只需要设置 $K_1=K_2$ 即可。单密钥 DES 的数学描述为：

$$C = E(P,K)$$

在 3DES 中，如果令 $K_1=K_2=K$，那么结果就与单密钥 DES 相同，数学描述为：

$$C = E(D(E(P,K),K),K) = E(P,K)$$

2.4.4 高级加密标准

由于 DES 存在的缺陷出现了 3DES，但 3DES 在应用中也难以避免类似于 DES 的厄运。为此，美国标准和技术委员会于 1997 年开始向世界各地的研究人员发起邀请，征集一个新的加密标准方案，这个方案就是高级加密标准(Advanced Encryption Standard，AES)。该加密标准要求具有以下功能特点。

(1) 必须是一个对称加密算法。

(2) 必须公开所有的算法设计。

(3) 必须支持 128 位、192 位和 256 位密钥长度。

(4) 可同时支持软件和硬件两种实现方式。

1. AES 的特点

1998 年 8 月，NIST 根据对算法的安全性、效率、简单性、灵活性和内存需求等方面的综合考虑，从收到的 15 个提案中确定了其中 5 个方案。通过对这 5 个方案的无记名投票表决，于 2001 年 10 月确定了 Rijndael 作为美国政府标准，并作为联邦信息处理标准 FIPS197 被正式发表。Rijndael 的发音为 Rhine Dale[rain deil]。

在 Rijndael 中，密钥长度和数据块长度可以单独选择，之间没有必然的联系。密钥和数据块的长度以 32 位为间隔递增，在 128 位～256 位之间。在具体实施中，AES 一般有两种方案：一种是数据块和密钥都为 128 位；另一种是数据块为 128 位，而密钥为 256 位。而原定的 192 位的密钥几乎不使用。在下面的内容中，主要以数据块和密钥都为 128 位来介绍。

与 DES 一样，AES 也是一种迭代分组密码，同样使用了多轮置换和替换操作，并且操作是可逆的。但与 DES 不同的是，AES 算法不是 Feistel 密码结构，AES 的操作轮数在 10～14 之间。其中当数据块和密钥都为 128 位时，轮数为 10。随着数据块和密钥长度的增加，操作轮数也会随之增加，最大值为 14。不过，在每一次操作中，DES 是直接以位为单位，而在 AES 中则以 8 位的字节为单位。这样做的目的是便于通过硬件和软件实现。AES 的每一轮操作包括如下 4 个函数。

- ByteSub(字节替换)。用一张称为“S 盒子”的固定表来执行字节到字节的替换。
- ShiftRow(行移位置换)。行与行之间执行简单的置换。
- MixColumn(列混淆替换)。列中的每一个字节替换成该列所有字节的一个函数。
- AddRoundKey(轮密钥加)。用当前的数据块与扩充密钥的一部分进行简单的 XOR 运算。

以上 4 个函数中，具体为 1 次置换 3 次替换。

2. Rijndael 的工作原理及过程

图 2-13 所示的是 Rijndael 的 state 与 rk 数组的工作示意图。其中，128 位(16B)的明文以字节的形式存储在 4×4 的矩阵中，具体存放在 state 数组中。如下所示：

$$\begin{bmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{10} & a_{11} & a_{12} & a_{13} \\ a_{20} & a_{21} & a_{22} & a_{23} \\ a_{30} & a_{31} & a_{32} & a_{33} \end{bmatrix}$$

在算法开始时，state 数组被初始化为 128 位的明文数据块，其中前 4 个字节被存放在 state 数组的第 0 列，接下来的 4 个字节被放在第 1 列，依此类推。然后在轮操作过程中的每一步，state 数组都要被修改，其中包括数组内部字节对字节的置换，以及数组内部字节的替换。在算法的最后，state 中的内容就是加密后输出的密文。

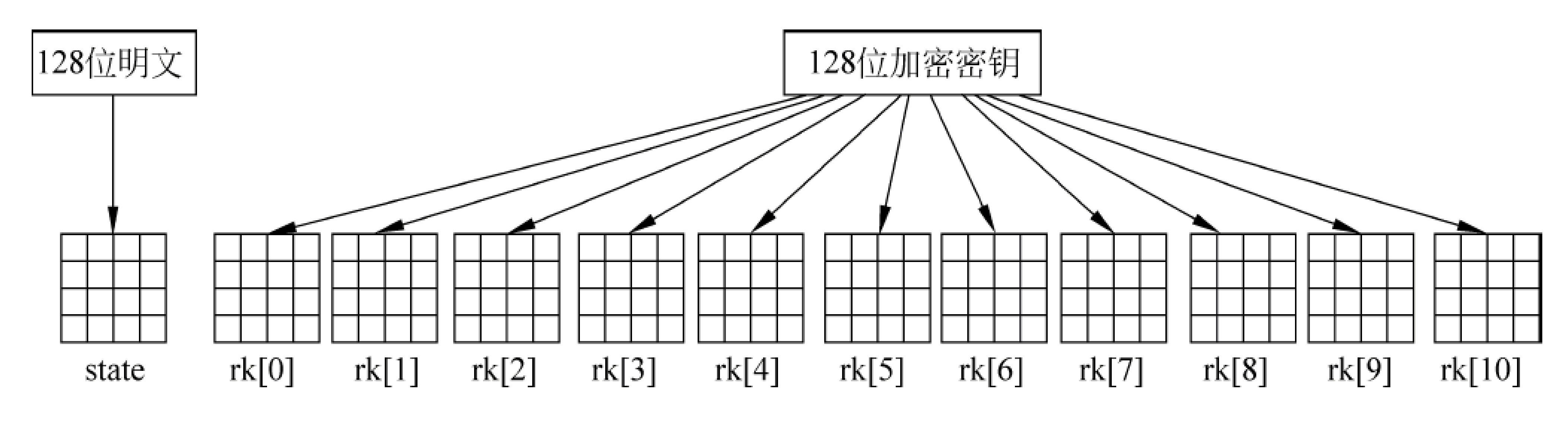


图 2-13　Rijndael 的 state 与 rk 数组的工作示意图

在进行 state 数组初始化的同时，128 位的密钥也被扩展到 11 个与 state 同样结构的状态数组 rk[i]中，i=0,1,2,…,10。rk 中存放的是由 128 位加密密钥扩展出的轮密码(也称为子密码)。其中，有一个 rk 被用在计算过程的开始处，其他 10 个 rk 被分别用在 10 轮计算中，每一轮使用一个数组。从 128 位的加密密钥扩展得到轮密码的过程基本上是通过反复地对密钥中的不同位进行循环移位和 XOR 运行生成的，具体实现非常复杂，在这里不再讨论。有兴趣的读者可以参考相关的文献资料。

在以下的介绍中，state 数组中已经存放了 128 位的明文。同时，假设由 128 位加密密钥扩展得到的轮密码已分别存放在数组 rk[i]中。

在开始轮操作之前，还需要进行一次 state 数组与 rk[0]数组之间的逐字节的 XOR 运算，结果存放在 state 数组中。即在进行轮操作之前，state 数组中每一个字节都被它与 rk[0]中对应的字节进行 XOR 运算后的结果取代。

接下来便进行主循环。这一循环将被执行 10 次，即进行 10 次迭代。在每一次迭代中都分别用 rk[i]与 state 之间的操作结果来替换 state 中的数据。每一轮的操作都需要经过以下 4 个步骤。

(1) 使用 ByteSub 操作，在 state 数组中进行逐字节的替换。令 state 中每个字节用 a_{ij} 表示，替换后的每一个字节用 b_{ij} 表示，则有 b_{ij}=ByteSub(a_{ij})，数学描述如下：

$$\begin{bmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{10} & a_{11} & a_{12} & a_{13} \\ a_{20} & a_{21} & a_{22} & a_{23} \\ a_{30} & a_{31} & a_{32} & a_{33} \end{bmatrix} \rightarrow \text{ByteSub} \rightarrow \begin{bmatrix} b_{00} & b_{01} & b_{02} & b_{03} \\ b_{10} & b_{11} & b_{12} & b_{13} \\ b_{20} & b_{21} & b_{22} & b_{23} \\ b_{30} & b_{31} & b_{32} & b_{33} \end{bmatrix}$$

在进行 ByteSub 操作时，实现方法与 DES 中的 S 盒子相似，可以直接通过查表(如图 2-14 所示)得到替换值。为便于表述，在图 2-14 中通过十六进制数来表示。例如，ByteSub(2e)=98，即在图 2-14 的表格中，第 2 列第 e 行对应的数值是 98。在 AES 和 DES

中虽然都使用了S盒子，但AES中的S盒子与DES中的不同，在DES中有8个S盒子，而在AES中只有一个。

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

图 2-14　ByteSub 的对照表

（2）对state数组中的每一个字节a_{ij}用ShiftRow操作向左进行行移位。将第(1)步操作得到的结果的行向左移位置换。具体方法为：第0行不变，第1行左移1个字节，第2行左移2个字节，第3行左移3个字节。这一步操作是通过ShiftRow将整个块中的数据混合起来，数学描述如下：

$$\begin{bmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{10} & a_{11} & a_{12} & a_{13} \\ a_{20} & a_{21} & a_{22} & a_{23} \\ a_{30} & a_{31} & a_{32} & a_{33} \end{bmatrix} \to \text{ShiftRow} \to \begin{bmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{11} & a_{12} & a_{13} & a_{10} \\ a_{22} & a_{23} & a_{20} & a_{21} \\ a_{33} & a_{30} & a_{31} & a_{32} \end{bmatrix}$$

（3）使用MixColumn操作将state数组中每一列的字节混合起来，列与列之间互不影响。这里的操作类似于DES中的S盒子，包括移位和XOR运算，可以通过查表(类似于如图2-14所示的表)实现。数学描述如下：

$$\begin{bmatrix} a_{0i} \\ a_{1i} \\ a_{2i} \\ a_{3i} \end{bmatrix} \to \text{MixColumn} \to \begin{bmatrix} b_{0i} \\ b_{1i} \\ b_{2i} \\ b_{3i} \end{bmatrix}, \quad \text{其中} \quad i = 0,1,2,3$$

（4）使用AddRoundKey操作，与本轮的轮密钥进行XOR运算，其结果保存到state数组中。与DES相似，密钥扩展算法产生每一轮的轮密钥，并保存在rk[i]中。为了表述方便，在这里用k_{ij}来代替rk[i]，但k_{ij}中的i和j分别表示存放轮密钥的矩阵的行和列($i,j=0,1,2,3$)，而rk[i]中的i则表示是第i轮使用的轮密钥($i=1,2\cdots,10$)。将轮密钥k_{ij}和当前4×4字节矩阵a_{ij}进行XOR操作生成b_{ij}的过程描述如下：

$$\begin{bmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{10} & a_{11} & a_{12} & a_{13} \\ a_{20} & a_{21} & a_{22} & a_{23} \\ a_{30} & a_{31} & a_{32} & a_{33} \end{bmatrix} \oplus \begin{bmatrix} k_{00} & k_{01} & k_{02} & k_{03} \\ k_{10} & k_{11} & k_{12} & k_{13} \\ k_{20} & k_{21} & k_{22} & k_{23} \\ k_{30} & k_{31} & k_{32} & k_{33} \end{bmatrix} = \begin{bmatrix} b_{00} & b_{01} & b_{02} & b_{03} \\ b_{10} & b_{11} & b_{12} & b_{13} \\ b_{20} & b_{21} & b_{22} & b_{23} \\ b_{30} & b_{31} & b_{32} & b_{33} \end{bmatrix}$$

通过以上 XOR 操作后，生成的 b_{ij} 再替换掉 state 中的 a_{ij}，这时 a_{ij} 就是加密后的密文。

在以上操作中，由于每一步都是可逆的，所以解密过程也非常简单，只要将加密算法反过来运行就可以实现。

2.4.5 其他分组密码算法

在分组密码算法中，本书重点介绍了 DES、3DES 和 AES。除此之外，本节将简要介绍几种重要的分组密码算法。

1. 国际数据加密算法

DES 加密标准的出现在密码学上具有划时代的意义，但比 DES 更安全的加密算法也在不断出现。除 3DES 外，另一个对称加密系统是国际数据加密算法（International Data Encryption Algorithm，IDEA）。

IDEA 的明文和密文都是 64 位，但密钥长度为 128 位，因而更加安全。IDEA 和 DES 相似，也是先将明文划分为一个个 64 位的数据块，然后经过 8 轮编码和一次替换，得出 64 位的密文。同时，对于每一轮的编码，每一个输出位都与每一个输入位有关。IDEA 比 DES 的加密性好，加密和解密的运算速度很快，无论是软件还是硬件，实现起来都比较容易。

2. RC5/RC6

RC5 和 RC6 分组密码算法是由 MIT（麻省理工学院）的 Ron Rivest 于 1994 年提出的，并由 RSA 实验室对其性能进行分析。RC5 适合于硬件和软件实现，只使用在微处理器上。RC5 的设计特性如下。

（1）快速。RC5 是面向字的，在基本操作中每次对数据的整个字进行处理。

（2）适用于不同字长的处理器。一个字中的位数作为 RC5 的一个参数，不同的字长使用不同的算法。

（3）可变的循环次数。循环次数是 RC5 的另一个参数，这个参数使 RC5 可以在更高的速度和更高的安全性之间进行折衷选择。

（4）可变长度的密钥。密钥长度是 RC5 的第 3 个参数，这个参数可以用来在更高的速度和更高的安全性之间进行折衷选择。

（5）结构简单。RC5 的结构简单，易于实现，并简化了确定算法的操作强度。

（6）内存要求低。由于 RC5 算法对设备内存的要求很低，所以可以应用在智能卡等有限内存的设备上。

（7）大量使用数据依赖循环。RC5 中移位的位数依赖于数据的循环操作，以加强算法对密码分析的抵抗能力。

RC5 已经被用于 RSA 的主要产品中，包括 BSAFE、S/MAIL 等。RC5 中使用的三个参数如表 2-1 所示。

表 2-1　RC5 算法中的三个参数说明

参数	定义	取值范围
w	字的大小，RC5 对两字分组进行加密	16,32,64
r	循环次数	0,1,2,…,255
b	密钥 K 中 8 位字节的个数	0,1,2,…,255

具体来说，RC5 可以将 32 位、64 位或 128 位长度的明文分组进行加密，生成同样长度的密文分组。使用的密钥长度为 0～2040 位，加密的循环次数可在 0～255 之间选择。所以，RC5 的一个特定的版本被写成 RC5-w/r/b，例如 RC5-32/12/16，即明文分组的字大小为 32 位(加密操作时为 64 位，32 位的明文和 32 位的密文分组)，加密和解密算法包含 12 次循环，密钥长度为 16 个字节(128 位)。Ron Rivest 建议把 RC5-32/12/16 作为指定版本使用。

RC6 是在 RC5 的基础上设计出来的。当 1997 年美国国家标准技术委员会征集 ADE 算法时，RSA 实验室想在 RC5 的基础上设计一种新密码，力争在满足 AES 要求的同时，还具有更简单的设计、更高的安全性和更好的性能。但在 2001 年公布的 AES 结果中，RC6 落选了。

RC6 继承了 RC5 的优点，并且为了符合美国国家标准技术委员会提出的分组长度为 128 位的要求，RC6 使用了 4 个寄存器，并加入了 32 位的整数乘法，用于加强扩展性。与 RC5 的表示一样，RC6 可以更精确地表示为 RC6-w/r/b，其中字长 w 为 32 位(与 RC5 相同)，加密轮数 r 为 20，加密密钥的字节数 b 为 16、24 或 32 字节。

3. TEA

TEA(Tiny Encryption Algorithm，微型加密算法)是由英国剑桥大学计算机实验室的 David J. Wheeler 和 Roger M. Needham 于 1994 年提出的一种对称分组密码算法。它采用 128 位的密钥对 64 位的数据分组进行加密，其循环次数可由用户根据加密强度需要设定。

在前面介绍的分组密码设计中，需要在每轮操作的复杂度和执行轮数之间进行折衷。其中，DES 在两者之间进行平衡，而 AES 减少了轮数却增加了轮函数的复杂度。TEA 使用非常简单的轮函数，它通过增加循环的轮数来提高算法的安全性。

由于 TEA 不是 Feistel 结构密码，所以需要设计加密和解密的程序，不过同时实现加密和解密的程序对 TEA 只需要几行代码。另一方面，由于 TEA 近似于 Feistel 结构密码，所以可使用加法和减法运算来代替 XOR 操作。TEA 在加密和解密过程中，加法运算和减法运算用作可逆的操作。算法轮流使用异或运算和加法运算提供非线性特性，双移位操作使密钥和数据的所有位重复地混合。

一般认为，32 轮循环就具备足够的加密强度。当循环次数达到 32 轮以上时，TEA 算法将具有很强的抗攻击能力。另外，由于 TEA 采用了 128 位的密钥，并且不存在 DES 算法中的 S 盒子问题，算法本身非常简练，所以无论采用软件方式还是硬件方式，实现起来都非常容易。因此，TEA 是一种较为优秀的对称分组密码算法。

其他的分组加密算法还有 LOKI、CAST-256、CRYPTON、E2、DEAL、FROG、SAFER＋、MAGENTA、SERPENT、MARS、DFC、Twofish 和 HPC 等。这 13 个算法都是 1998 年公布的 AES 中的候选算法，另两个是前面介绍的 RC6 和 Rijndael。

2.5 非对称加密

非对称加密也称为公钥加密。在对称加密系统中，加密和解密的双方使用的是相同的密钥。在实际情况下，怎么才能实现加密和解密的密钥一致呢？一般有两种方式：事先约定和用信使来传送。如果加密和解密的双方对密钥进行了事先约定，就会给密钥的管理和更换带来极大的不便；如果使用信使来传送密钥，很显然是不安全的。另一种可行的方法是通过密钥分配中心(Key Distribution Center，KDC)来管理密钥，这种方法虽然安全性较高，但所需要的成本也会增大。而非对称加密可以解决此问题。

2.5.1 非对称加密概述

非对称加密的出现在密码学史上是一个重要的里程碑。非对称加密中使用的公开密钥(或公钥密钥)的概念是在解决对称加密的单密码方式中最难解决的两个问题时提出的，这两个问题是：密钥分配和数字签名。

在使用单钥密码进行加密通信时，对于密钥的分配和管理一般有两种方式：一种是通信双方拥有一个共享的密钥；另一种是借助于一个密钥分配中心。如果是前者，可用人工方式传送双方的共享密钥，其成本较高，而且安全性要依赖于信使的可靠性。如果是后者，则完全依赖于密钥分配中心的可靠性。第二个问题是数字签名。考虑的是如何对数字化的消息或文件提供一种类似于书面文件的手书签名方式。1976 年，W. Diffice 和 M. Hellman 为解决以上问题，提出了公钥密码体制。

在非对称加密体系中，密钥被分解为一对，即公开密钥和私有密钥。这对密钥中的任何一把都可以作为公开密钥(加密密钥)通过非保密方式向他人公开，而另一把作为私有密钥(解密密钥)加以保存。在加密系统中，公开密钥用于加密，私有密钥用于解密。私有密钥只能由生成密钥的交换方掌握，公开密钥可广泛公布，但它只对应于生成密钥的交换方。

非对称加密算法具有如下特点。

(1) 用公开密钥加密的数据(消息)，只有使用相应的私有密钥才能解密。这一过程称为加密。

(2) 使用私有密钥加密的数据(消息)，也只有相应的公开密钥才能解密。这一过程称为数字签名。

如图 2-15 所示，如果某一用户要给用户 A 发送一个数据，这时该用户会在公开的密钥中找到与用户 A 所拥有的私有密钥对应的一个公开密钥，然后用此公开密钥对数据进行加密后发送到网络中传输。用户 A 在接收到密文后便通过自己的私有密钥进行解密，因为数据的发送方使用接收方的公开密钥来加密数据，所以只有用户 A 才能够读懂该密文。当其他用户获得该密文时，因为他们没有加密该信息的公开密钥对应的私有密钥，所以无法读懂该密文。

在非对称加密中，所有参与加密通信的用户都可以获得每个用户的公开密钥，而每一个用户的私有密钥由用户在本地产生，不需要被事先分配。在一个系统中，只要能够管理好每一个用户的私有密钥，用户收到的通信内容则是安全的。任何时候，一个系统都可以更改它的私有密钥，并公开相应的公开密钥来替代它原来的公开密钥。

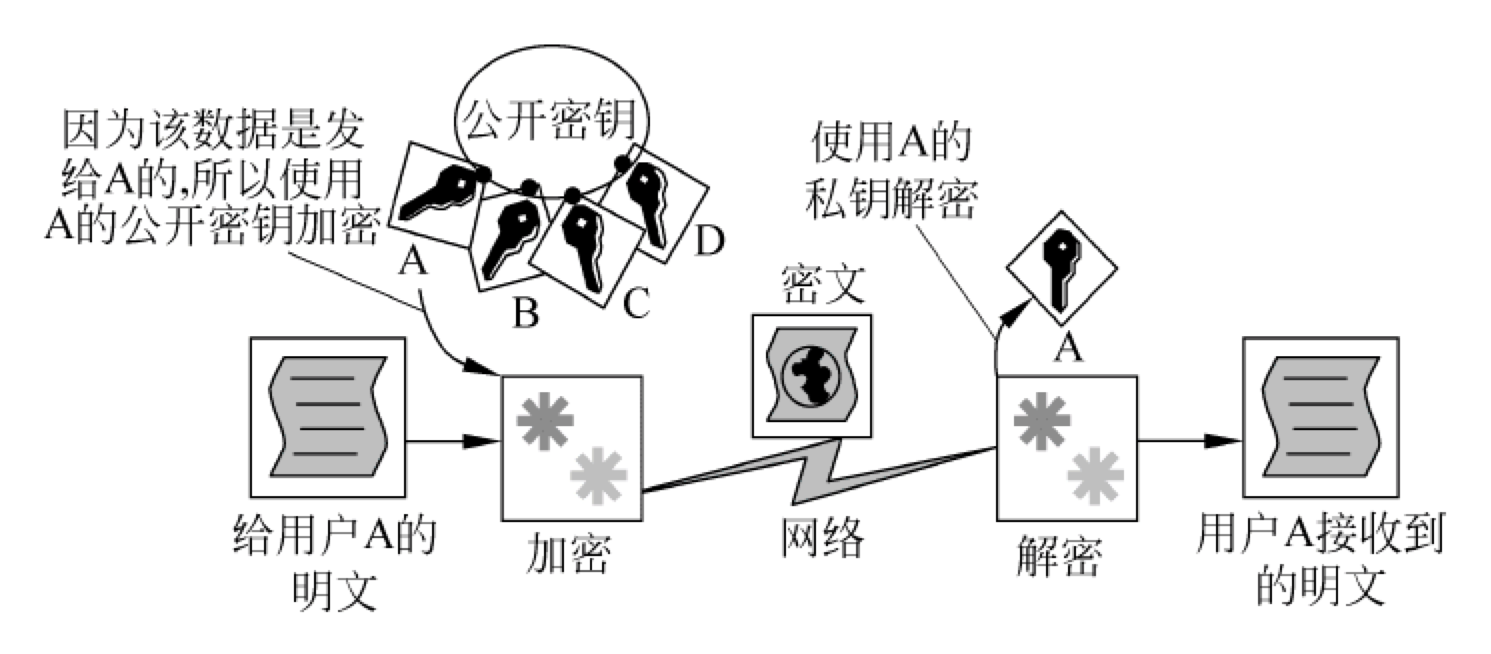


图 2-15　非对称密钥的加密和解密过程

非对称加密方式可以使通信双方无需事先交换密钥就可以建立安全通信，广泛应用于身份认证、数字签名等信息交换领域。公开密钥体系是基于“单向陷门函数”的，即一个函数正向计算是很容易的，但是反向计算则是非常困难的。陷门的目的是确保攻击者不能使用公开的信息得出秘密的信息。例如，计算两个质数 p 和 q 的乘积 $n=pq$ 是很容易的，但是要分解已知的 n 成为 p 和 q 是非常困难的。

遵循业界的约定，本章在介绍对称加密时，明文为 P，密文为 C。而在非对称加密中，用 M(也可以用 P)表示要加密的信息，加密结果仍然用 C 表示。

2.5.2　RSA

RSA(RSA 即三个发明人名字的第一个字母)算法是 Rivest、Shamir 和 Adleman 于 1977 年提出的第一个完善的公开密钥算法，其安全性是基于分解大整数的困难性。在 RSA 算法中使用了这样一个基本事实：到目前为止，无法找到一个有效的算法来分解两个大质数之积。

1. RSA 的原理

RSA 公开密钥算法的原理如下。

① 选择两个互异的大质数 p 和 q(p 和 q 必须保密，一般取 1024 位)。

② 计算出 $n=pq$，$z=(p-1)(q-1)$。

③ 选择一个比 n 小且与 z 互质(没有公因子)的数 e。

④ 找出一个 d，使得 $ed-1$ 能够被 z 整除。其中，$ed=1 \bmod (p-1)(q-1)$。

⑤ 因为 RSA 是一种分组密码系统，所以公开密钥$=(n,e)$，私有密钥$=(n,d)$。

在以上的关系式中，n 称为模数，通信双方都必须知道；e 为加密运算的指数，发送方需要知道；而 d 为解密运算的指数，只有接收方才能知道。

将以上的过程进一步描述如下。

公开密钥：$n=pq$(p、q 分别为两个互异的大素数，p、q 必须保密)，e 与$(p-1)(q-1)$互质。

私有密钥：$d=e^{-1}\{\bmod (p-1)(q-1)\}$。

加密：$C=M^e(\bmod n)$，其中 M 为明文，C 为密文。

解密：$M=C^d(\bmod n)=(M^e)^d(\bmod n)=M^{ed}(\bmod n)$。

2. RSA 应用举例

为了对字母表中的第 M 个字母加密，加密算法为 $C=M^e(\bmod n)$，第 C 个字母即为加密后的字母。对应的解密算法为 $M=C^d(\bmod n)$。下面以一个简单的例子进行计算。

① 设 $p=5$，$q=7$。

② 所以 $n=pq=35$，$z=(5-1)(7-1)=24$。

③ 选择 $e=5$(因为 5 与 24 互质)。

④ 选择 $d=29$($ed-1=144$，可以被 24 整除)。

⑤ 所以公开密钥为(35,5)，私有密钥为(35,29)。

如果被加密的是 26 个字母中的第 12 个字母(L)，则它的密文为：

$$C = 12^5 (\text{mod } 35) = 17$$

第 17 个字母为 Q，解密得到的明文为：

$$M = 17^{29} (\text{mod } 35) = 12。$$

通过以上的计算可以看出，当两个互质数 p 和 q 取的值足够大时，RSA 的加密是非常安全的。

2.5.3 其他非对称加密算法

在非对称加密算法中，除前面介绍的 RSA 外，还有 DH 算法和椭圆曲线密码等，以下进行简要介绍。

1. DH 算法

DH(Diffie-Hellman)算法是一种“密钥交换”算法，它主要为对称密码的传输提供共享信道，而不是用于加密或数字签名。

DH 的数学描述相对简单。令 p 为质数，g 为生成元，即对于任意 $x\in\{1,2,3,\cdots,p-1\}$，可以找到指数 n，使得 $x=g^n \bmod p$。其中，p 的值和生成元 g 是公开的。现在为了实现密钥交换，用户 A 生成他的密钥指数 a，用户 B 生成他的密钥指数 b。用户 A 发送($g^a \bmod p$)给用户 B，用户 B 发送($g^b \bmod p$)给用户 A。于是用户 A 计算：

$$(g^b)^a \bmod p = g^{ab} \bmod p$$

用户 B 计算：

$$(g^a)^b \bmod p = g^{ab} \bmod p$$

于是($g^{ab} \bmod p$)就是用于共享信道的对称密钥。DH 密钥的交换过程如图 2-16 所示。

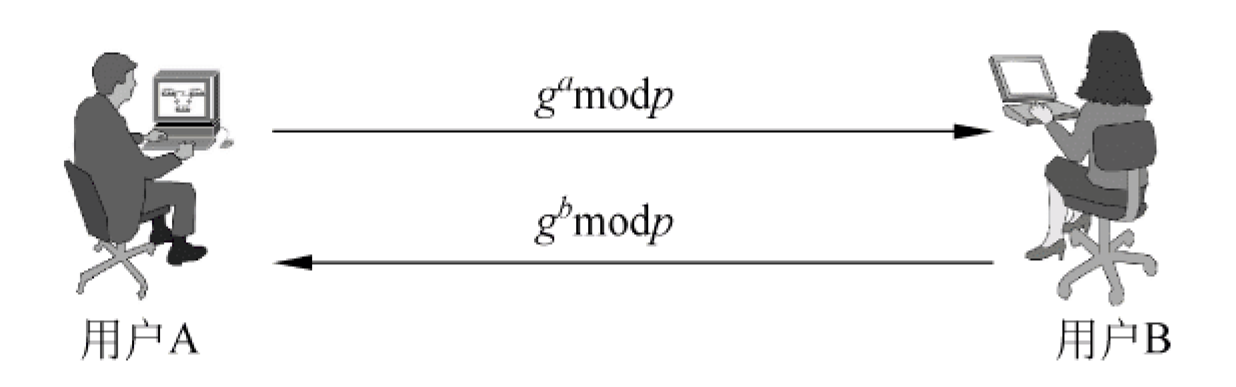


图 2-16　DH 密钥交换方式

2. 椭圆曲线密码

椭圆曲线密码(Elliptic Curve Cryptography，ECC)是自 RSA 后出现的一个有竞争力的公开密钥算法。椭圆曲线密码系统的安全强度不但依赖于在椭圆曲线上离散对数的分解难度，也依赖于曲线的选择。

椭圆曲线离散对数问题(ECDLP)是椭圆曲线密码学的基础。椭圆曲线离散对数问题可描述如下：给定(或根据某一法则构造)一条椭圆曲线 E，并在曲线上取一点 P，并用 xP 表示点 P 与自身相加 x 次，即 xP=P+P+…+P，共有 x 个 P 相加。假设曲线 E 上有一点 Q，使得 Q=xP 成立，那么椭圆曲线离散对数问题就是给定点 P 和点 Q，求解 x 的问题。下

面是 ECC 的 ECDLP 算法。

(1) 系统的建立。选取一个基域 F_q,一个定义在 F_q 上的椭圆曲线 E 和 E 上一个为质数阶 n 的点 P,点 P 的坐标用 (x_p, y_p) 表示。有限域 F_q、椭圆曲线参数(即域元素 a 和 b,元素 a 和 b 用于定义椭圆曲线的参数)、点 P 和阶 n 是公开的。

(2) 密钥的生成。系统建成后,通信双方执行下列计算。

① 在区间 $[1, n-1]$ 中随机选取一个整数 d。

② 计算点 $Q = dP$。

③ 用户的公开密钥包含点 Q,用户的私有密钥是整数 d。

(3) 加密过程。假设,当用户 B 发送信息 M 给用户 A 时,用户 B 将执行下列操作。

① 查找用户 A 的公钥 Q。

② 将数据 M 表示成一个域元素 M。

③ 在区间 $[1, n-1]$ 内选择一个随机整数 k。

④ 计算点 $(x_1, y_1) = kP$。

⑤ 计算点 $(x_2, y_2) = kQ$,如果 $x_2 = 0$,则回到第③步。

⑥ 计算 $c = Mx_2$。

⑦ 传送加密数据 (x_1, y_1, c) 给用户 A。

(4) 解密过程。当用户 A 解密从用户 B 收到的密文 (x_1, y_1, c) 时,用户 A 执行下列操作。

① 使用用户 A 的私有密钥 d,计算点 $(x_2, y_2) = d(x_1, y_1)$。

② 通过计算 $M = c/x_2$,得到明文数据 M。

(5) ECC 的特点。基于离散对数问题的椭圆曲线密码体制有两方面的特点:一方面,它把实数域上的乘法运算、指数运算等映射成椭圆曲线上的加法运算。无论是用硬件实现还是用软件实现,都比其他公开密钥体系更快,更容易实现,成本更低。另一方面,在有限数域的椭圆曲线上要求出上面的 d,同时涉及到整数因式分解问题和离散对数问题,解决这些问题的难度在很大程度上增加了 ECC 的安全性。

2003 年 5 月 12 日中国颁布的无线局域网国家标准 GB15629.11 中,包含了全新的 WAPI(WLAN Authentication and Privacy Infrastructure)安全机制,其中用到的数字签名就采用了 ECC 算法。另外,国际上最著名的 ECC 密码技术公司加拿大 Certicom 公司已授权 300 多家企业使用 ECC 密码技术,包括 Cisco 系统有限公司、摩托罗拉等企业。Microsoft 公司将 Certicom 公司的 VPN 嵌入到 Windows Server 2003 操作系统中。

2.6 数字签名

多少年来,人们一直在根据亲笔签名或印章来鉴别书信或文件的真实性。但随着基于计算机网络所支持的电子商务、网上办公等平台的广泛应用,原始的亲笔签名和印章方式已无法满足应用需要,因此数字签名技术应运而生。

2.6.1 数字签名的概念和要求

数字签名(digital signature)在 TS07498-2 标准中的定义为:"附加在数据单元上的一些数据,或是对数据单元所作的密码变换。这种数据和变换允许数据单元的接收者用以确

认数据单元来源和数据单元的完整性，并保护数据，防止被人（例如接收者）伪造。"数字签名必须同时满足以下的要求。

（1）发送者事后不能否认对报文的签名。

（2）接收者能够核实发送者发送的报文签名。

（3）接收者不能伪造发送者的报文签名。

（4）接收者不能对发送者的报文进行部分篡改。

（5）网络中的其他用户不能冒充成为报文的接收者或发送者。

数字签名是实现安全认证的重要工具和手段，它能够提供身份认证、数据完整性和不可抵赖等安全服务。

（1）防冒充（伪造）。其他人不能伪造对消息的签名，因为私有密钥只有签名者自己知道和拥有，所以其他人不可能构造出正确的签名数据。

（2）可鉴别身份。接收者使用发送者的公开密钥对签名报文进行解密运算，并证明对方身份是真实的。

（3）防篡改。即防止破坏信息的完整性。签名数据和原有文件经过加密处理已形成了一个密文数据，不可能被篡改，从而保证了数据的完整性。

（4）防抵赖。数字签名可以鉴别身份，不可能冒充伪造。

数字签名是附加在报文（数据或消息）上并随报文一起传送的一串代码，与传统的亲笔签名和印章一样，目的是让接收方相信报文的真实性，必要时还可以对真实性进行鉴别。现在已有多种数字签名的实现方法，但采用较多的还是技术上非常成熟的数据加密技术，其中既可以采用对称加密，也可以采用非对称加密，但非对称加密要比对称加密更容易实现和管理。

2.6.2 利用对称加密方式实现数字签名

读者已经知道，对称加密在通信过程中存在一定的缺陷，主要是密钥的交换比较困难。在对称加密中，由于加密密钥和解密密钥是相同的，如果将其用于数字签名，则要求消息的发送者和接收者都要使用相同的密钥。发送者用密钥对消息进行加密处理（签名）生成密文，接收者对接收到的密文利用同一个密钥进行解密。在这一过程中，读者会发现违反了数字签名的一个原则：防抵赖。由于在加密（签名）和解密（鉴别身份）过程中，参与者只有消息的发送方和接收方，而没有第三方，一旦出现签名的抵赖，则无法进行判别。

为解决这一问题，在利用对称加密方式实现数字签名的过程中，需要一个大家共同依赖的权威机构作为第三方。数字签名的用户都要向该权威机构申请一个密钥，这个密钥在该系统中是唯一的，即唯一标识了某一个用户。当权威机构向用户分配了密钥后，将该密钥的副本保存在该机构的数据库中，用以识别用户的真实性。

现在，假设用户 A 和用户 B 之间要实现数字签名，具体过程如下（如图 2-17 所示）。

（1）用户 A 对要发送的明文消息 P 进行签名处理，生成 $K_A(B,R_A,t,P)$。其中，K_A 是用户 A 的加密密钥，即从权威机构申请到的密钥；B 是用户 B 的标识，在网络上是公开的；R_A 是用户 A 选择的一个随机数，以防止用户 B 收到重复的签名消息；t 是一个时间戳，用来保证该消息是最新的；P 是用户 A 要发送的明文消息。

（2）用户 A 将利用自己的密钥加密生成的签名消息 $K_A(B,R_A,t,P)$ 发送出去，当权威机构接收到该消息后，通过数据库中用户 A 的密钥副本 K_A 知道该消息是用户 A 发送的，

所以将利用密钥副本 K_A 进行解密处理，得到用户 A 发送的明文 P。并根据用户的标识符知道该消息是发送给用户 B 的。

(3) 权威机构利用用户 B 的密钥副本 K_B 生成消息 $K_B(A,R_A,t,P,K_C(A,t,P))$。其中 $K_C(A,t,P)$ 是一条由权威机构经过签名的消息，一旦将来出现抵赖，则可以通过该消息来证明。

(4) 用户 B 在接收到消息 $K_B(A,R_A,t,P,K_C(A,t,P))$ 后，利用自己的密钥 K_B 解密得到用户 A 发送的明文。

在如图 2-17 所示的数字签名方式中，系统的安全性主要决定于两个方面：一是用户密钥保存中的安全性；二是权威机构的可信赖性。

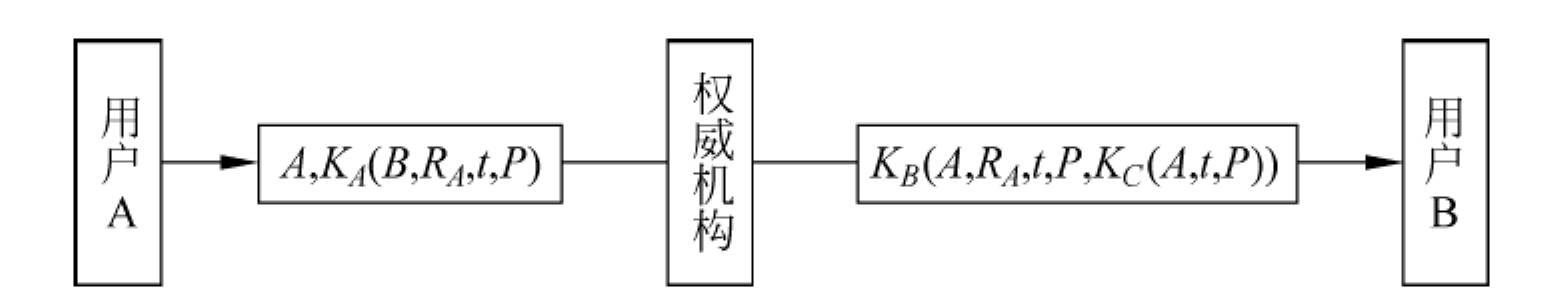


图 2-17　利用对称加密实现数字签名

2.6.3　利用非对称加密方式实现数字签名

在利用对称加密实现的数字签名中，用户必须依赖第三方的权威机构，所以权威机构的可信任度是决定该方式能否正常使用的关键。然而，非对称加密解决了这一问题。

利用非对称加密方式实现数字签名，主要是基于在加密和解密过程中 $D(E(P))=P$ 和 $E(D(P))=P$ 两种方式的同时实现，其中前面介绍的 RSA 算法就具有此功能。

具体实现过程如图 2-18 所示，首先发送方利用自己的私有密钥对消息进行加密(这次加密的目的是实现签名)，接着对经过签名的消息利用接收方的公开密钥再进行加密(这次加密的目的是保证消息传送的安全性)。这样，经过双重加密后的消息(密文)通过网络传送到接收方。接收方在接收到密文后，首先利用接收方的私有密钥进行第一次解密(保证数据的完全性)，接着再用发送方的公开密钥进行第二次解密(鉴别签名的真实性)，最后得到明文。

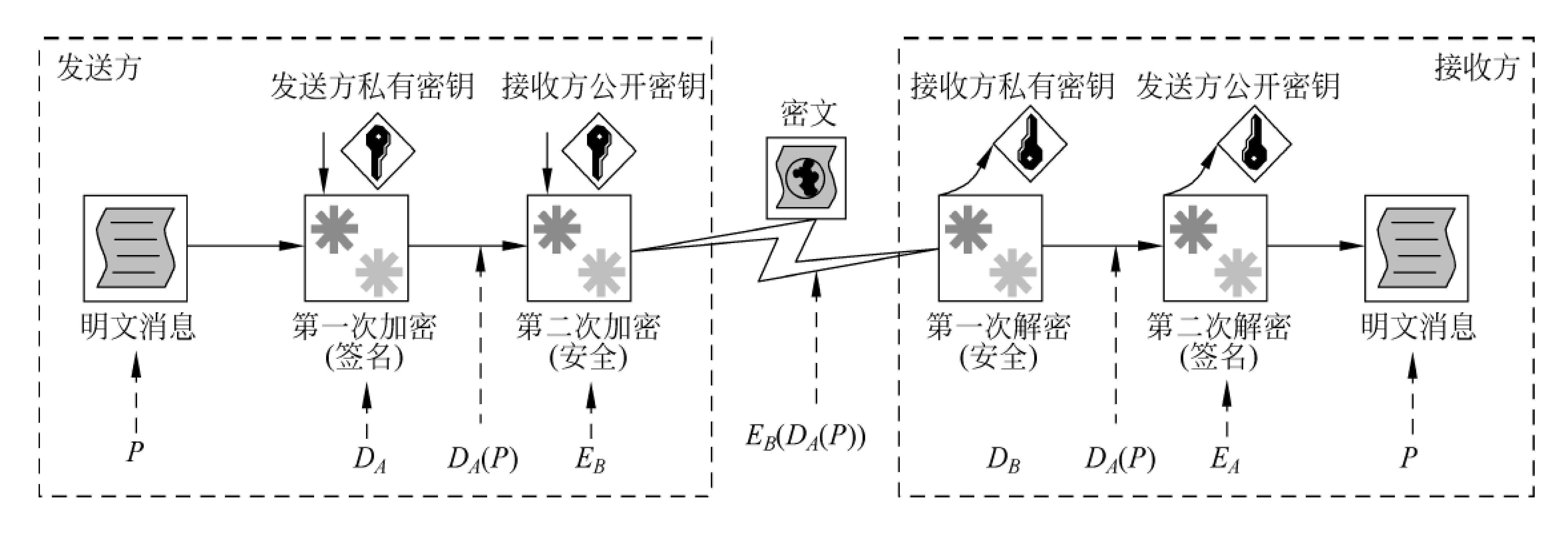


图 2-18　具有保密功能的数字签名实现过程

现在，假设发送方否认自己给接收方发送过消息 P。这时，接收方只需要同时提供 P 和 $D_A(P)$。第三方可对接收方提供的 $D_A(P)$ 利用 E_A 进行解密，即 $E_A(D_A(P))$。由于 $D_A(P)$ 是由发送方使用自己的私有密钥签名的，而 E_A 是发送方的公开密钥，第三方很容易

得到且不需要发送方的许可。如果 $E_A(D_A(P))=P$,则说明该消息肯定是发送方发送的,因为只有发送方才有签名密钥 D_A。

2.7 报文鉴别

报文鉴别(message authentication)是在信息领域防止各种主动攻击(如信息的篡改与伪造)的有效方法。报文鉴别要求报文的接收方能够验证所收到的报文的真实性,包括发送者姓名、发送时间和发送内容等。

2.7.1 报文鉴别的概念和现状

报文鉴别也称"报文认证"或"消息认证",是一个证实收到的报文来自可信任的信息源且未被篡改的过程。报文鉴别也可用于证实报文的序列编号和及时性,因此利用报文鉴别方式可以避免以下现象的发生。

(1) 伪造消息。攻击者伪造消息发送给目标端,却声称该消息源来自一个已授权的实体(如计算机或用户),或攻击者以接收者的名义伪造假的确认报文。

(2) 内容篡改。以插入、删除、调换或修改等方式篡改消息。

(3) 序号篡改:在像 TCP 等依赖报文序列号的通信协议中,对通信双方的报文序号进行修改,包括插入、删除和重排序号等。这在目前的网络攻击事件中很常见。

(4) 记时篡改。篡改报文的时间戳以达到报文延迟或重传的目的。

产生报文鉴别符的方法可归纳为三种:一是对报文进行加密,以整个报文的密文作为鉴别符;二是用消息认证码(Message Authentication Code,MAC),该算法使用一个密钥,以报文内容为输入,产生一个较短的定长值作为鉴别符;三是用哈希(Hash)函数,也叫散列函数或杂凑函数,是一个将任意长的报文映射为定长 Hash 值的公共函数,以 Hash 值作为鉴别符。

目前,像对称加密、非对称加密等常规的加密技术已十分成熟,但出于多种原因,常规加密技术没有被简单地应用到报文鉴别符,实际应用中一般采用独立的报文鉴别码。目前,用避免加密的方法提供报文鉴别越来越受到重视。在最近几年,报文鉴别研究的热点转向由 Hash 函数导出 MAC。

2.7.2 Hash 函数

Hash 函数是一种能够将任意长度的消息压缩到某一固定长度的消息摘要(message digest)的函数。Hash 函数的基本思想是把其函数值看成输入报文的报文摘要,当输入中的任何一个二进制位发生变化时都将引起 Hash 函数值的变化,其目的就是要产生文件、消息或其他数据块的"指纹"。密码学上的 Hash 函数能够接受任意长的消息为输入,并产生定长的输出。为了满足报文鉴别的数据完整性需要,Hash 函数 $H()$必须满足以下特点。

(1) 效率。对于任意给定的输入 x,计算 $y=H(x)$要相对容易。并且,随着输入 x 长度的增加,虽然计算 $y=H(x)$的工作量会增加,但增加的量不会太快。

(2) 压缩。对于任意给定的输入 x,都会输出固定长度的 $y=H(x)$,且 y 要比 x 小得多。

(3) 单向性。对于给定的任意值 y,寻找一个 x,且使得 $H(x)=y$ 在计算上不可行。

(4) 弱抗碰撞。对于任意给定的 x 和 $H(x)$,寻找 y,且 $y\neq x$,使得 $H(x)=H(y)$在计算上不可行。

(5) 强抗碰撞。寻找任意的 x 和 y,并且 $y\neq x$,使得 $H(x)=H(y)$在计算上是不可行的。

其中,第 1 个性质可以看作是 Hash 函数用作报文鉴别的实际应用需求,对于后 4 条性质,是针对 Hash 函数在应用中的安全性而特别提出的要求。

2.7.3 报文鉴别的一般实现方法

Hash 函数可以分为两类:带密钥的 Hash 函数和不带密钥的 Hash 函数。使用没有密钥的 Hash 码作为报文鉴别码的体制是不安全的,容易遭受到一些攻击。带密钥的 Hash 函数通常可以用来产生报文的鉴别码,对于通信双方之间传输的任何消息 m,用带密钥的 Hash 函数 $H()$对 m 做变换,产生 $H(m)$作为 MAC 附于报文 m 之后,保证通信双方之间消息的完整性,使双方之间的消息没有被第三方篡改或伪造。常用的报文鉴别的实现需要加密技术。目前,实际应用的报文鉴别系统的具体实现过程如下所示。

① 发送方和接收方首先要确定一个固定长度的报文摘要 $H(m)$。

② 发送方通过 Hash 函数将要发送的报文 m“嚼碎”为报文摘要 $H(m)$。

③ 发送方对报文摘要 $H(m)$进行加密,得到密文 $E_k(H(m))$。

④ 发送方将 $E_k(H(m))$追加到报文 m 后面发送给接收方。

⑤ 接收方在成功接收到 $E_k(H(m))$和报文 m 后,先对 $E_k(H(m))$进行解密得到 $H(m)$,然后再对报文 m 进行同样的报文摘要运算得到报文摘要 $H'(m)$。

⑥ 接收方对 $H(m)$和 $H'(m)$进行比较,如果结果是 $H(m)=H'(m)$,可以断定收到的报文 m 是真实的。否则报文 m 在传送中被进行了篡改或伪造。

由以上的实现过程可以看出,不管传输的报文 m 有多大,其报文摘要 $H(m)$是不变的。同时,系统仅对报文摘要 $H(m)$进行加密和解密操作,报文 m 是以明文方式传送。另外,报文摘要算法的特点也很简单:两个不同的报文 m 不可能产生同一个报文摘要 $H(m)$。所以,这种鉴别方式对系统的要求较低,很适合 Internet 网络的应用。

2.7.4 报文摘要 MD5

MD5 是 Ronald Rivest 设计的一系列消息摘要算法中的第 5 个算法,其前一个版本的算法是 MD4。在 RFC 1321 中规定的报文摘要 MD5 算法已经得到了广泛应用。MD5 算法的特点是可以对任意长度的报文进行运算,得到的报文摘要长度均为 128 位。

MD5 算法的输入是一个“字节串”(而非“字符串”),每个字节为 8 位,所以下面的介绍以字节为单位进行说明。MD5 算法的原理如图 2-19 所示,具体过程如下。

① 填充。MD5 算法先对输入的数据进行填充补位,使得数据的长度(以 B 为单位)对 64 求余的结果是 56。即数据扩展至长度 $\text{Len}=k\times64+56$ 个字节,其中 k 为正整数。具体填充方法为:第一个位是 1,其他位全部为 0,直到满足上述要求。这一步总共补充的字节数为 0~63 个。

② 添加数据长度。用一个 8 字节(64 位)的整数表示数据的原始长度,将这个数字的 8

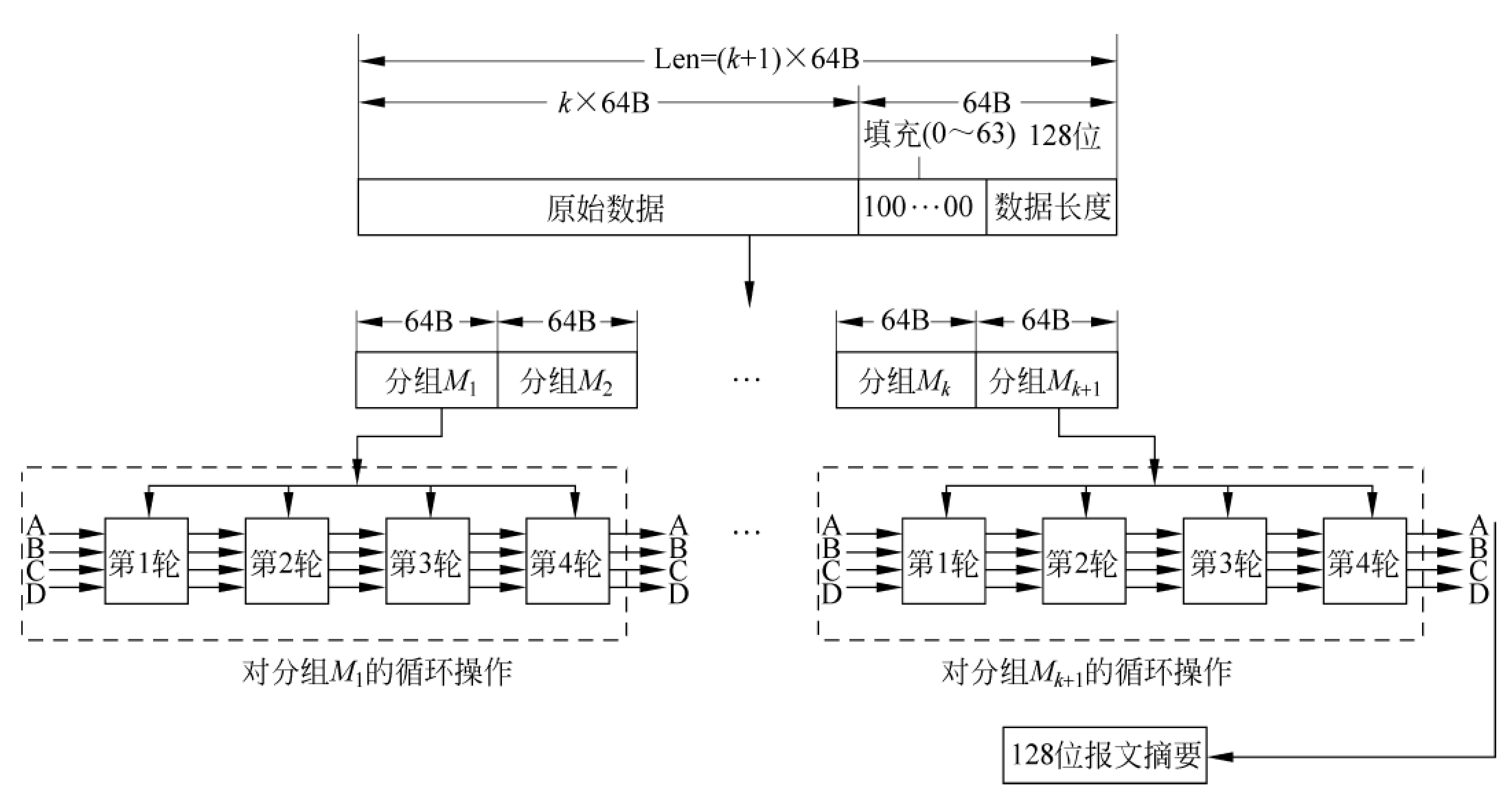


图 2-19　MD5 算法原理

个字节按低位在前，高位在后的顺序附加在"填充"位后的"数据长度"后面。这时，整个数据的长度：Len$=k\times64+56+8=(k+1)\times64$，单位为 B。

③ 初始化 MD5 缓存。使用一个 128 位的缓存来存放该 Hash 函数的中间变量及最终结果。该缓存被设置为由 4 个 32 位的寄存器(A、B、C 和 D)组成。这 4 个寄存器变量的初始值如下(以十六进制数表示的数值)。

A：01 23 45 67

B：89 ab cd ef

C：fe dc ba 98

D：76 54 32 10

④ 处理每一个 64 字节(512 位)的分组。算法的核心是一个包含 4 个循环的压缩函数，4 个循环有相似的结构，但每一次循环使用不同的原始逻辑函数 F()、G()、H()和 I()。

F(X,Y,Z)=(X and Y)or(not(X)and Z)

G(X,Y,Z)=(X and Z)or(Y and not(Z))

H(X,Y,Z)=X xor Y xor Z

I(X,Y,Z)=Y xor(X or not(Z))

其中，X、Y、Z 为 32 位整数。and 表示按位与，or 表示按位或，not()表示按位取反，xor 表示按位异或。

以上过程，从第一个分组(M_1)开始，每一个分组都要执行 4 轮操作。这一过程不断进行，直至所有的输入分组(共 $k+1$ 个)都被执行完毕。

⑤ 输出报文摘要。所有 $k+1$ 个以 64 字节为单位的分组处理完成后，最后产生的输出结果便是 128 位的报文摘要。

由此可以看出，MD5 算法中每一个输出位都要受到每一个输入位的影响，所以 MD5 可以有效防止消息被篡改，保证了消息的原始性和完整性。目前，MD5 算法已经较为完善，大部分编程语言(环境)都提供了 MD5 算法的实现，在很多应用系统中 MD5 已被确定为标准使用。

2.7.5 安全散列算法

MD5 目前的应用已经很广泛。另一个应用较为广泛的标准是由美国国家标准技术委员会提出的安全散列算法(Secure Hash Algorithm,SHA)。安全散列标准(SHS)于 1992 年 1 月 31 日在美国联邦记录中公布,1993 年 5 月 11 日起作为标准。1995 年 4 月 17 日公布了修改后的版本。SHA 是用于 SHS 的算法。

SHA 与 MD5 在总体实现思路上很相似,也是以任意长度的报文作为输入,并按 512 位长度的数据块进行处理。实际上,SHA 是 MD4 的一种变形。SHA 与 MD5 的主要区别如下。

(1) SHA 产生的报文摘要长度为 160 位,而 MD5 为 128 位。

(2) SHA 每轮有 20 步操作运算,而 MD5 仅有 4 轮。

(3) 所使用的运算函数不同。

SHA 比 MD5 更安全,但 SHA 对系统的要求较高。目前较新的版本为 SHA-1。

2.8 密钥的管理

在加密技术中,加密算法是公开的,而产生的密钥却要进行安全管理。密钥管理包括密钥的产生、分配、使用和验证等环节,其中密钥的分配和维护是非常重要的。

2.8.1 对称加密系统中的密钥管理

对称加密的一个缺点是密钥分配和管理非常复杂。对于每个加密设备,都需要使用单独的密钥,这时如果这个加密设备有多个联系对象,每个联系对象都必须拥有一个密钥。这时,就需要采取一定的方法将密钥分配给每一个联系对象。很显然,不管是采取人工方式还是网络分发(如通过加密的邮件进行群发)方式,所涉及的安全问题都是很明显的。

美国麻省理工学院开发了著名的密钥分配协议 Kerberos。Kerberos 协议通过使用密钥管理中心(Key Distribution Center,KDC)来分配和管理密钥。图 2-20 所示的是利用 KDC 进行密钥管理的一种实施方案,用户 A 和 B 都是 KDC 的注册用户,注册密钥分别为 K_a 和 K_b,密钥分配需要三个步骤(图中分别用①、②和③表示)。

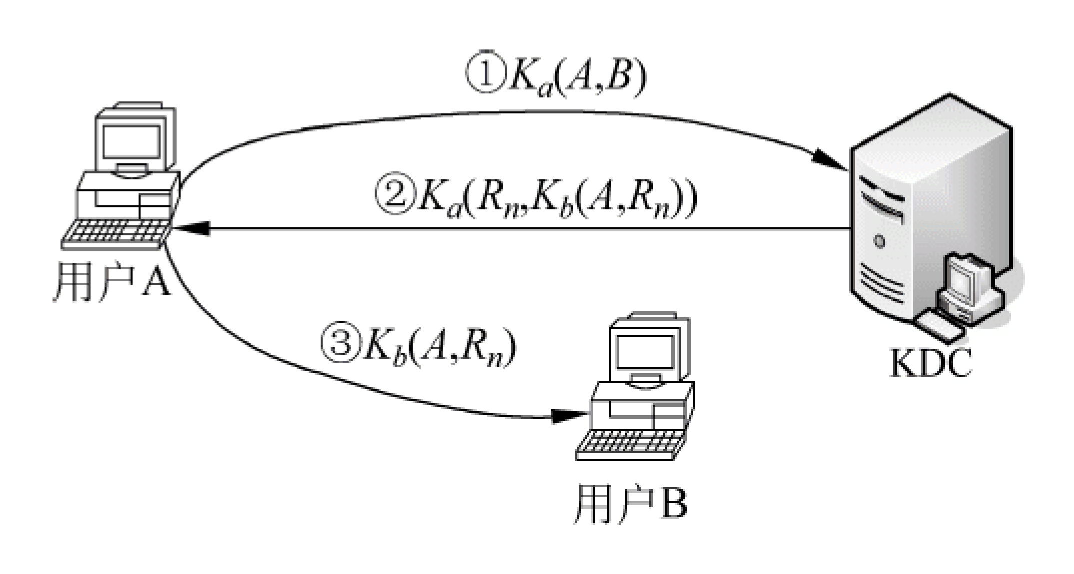


图 2-20 利用 KDC 管理密钥的一种方案

① 用户 A 向 KDC 发送用自己的注册密钥 K_a 加密的报文 $K_a(A,B)$,告诉 KDC 希望与用户 B 建立通信关系。

② KDC 随机地产生一个临时密钥 R_n,供用户 A 和 B 在本次通信中使用。然后向 A 发送应答报文,报文中包括 KDC 分配的临时密钥 R_n 和 KDC 请 A 转给 B 的报文 $K_b(A,R_n)$。此报文再用 A 自己的注册密钥 K_a 进行加密(因为是对称加密)。需要说明的是,虽然 KDC 向 A 发送了用 B 的注册密钥加密的报文 $K_b(A,R_n)$,但由于 A 并没有 B 的注册密钥,所以 A 根本无法知道明文的内容。

③ 用户 B 收到 A 转来的报文 $K_b(A,R_n)$时，一方面知道 A 要与自己通信，另一方面知道本次通信中使用的密钥是 R_n。

此后，用户 A 与 B 之间就可以利用密钥 R_n 进行通信了。由此可以看出，KDC 每次分配给用户的对称密钥是随机的，所以保密性较高。另外，KDC 分配给每个注册用户的密钥（如 K_a、K_b 等）都可以定期更新，以增加系统的安全性。

2.8.2 非对称加密系统中的密钥管理

在非对称加密系统中，如果某一用户知道其他用户的公开密钥就可以实现安全通信。在非对称加密系统中为了实现对密钥的管理，一般可通过一个值得依赖的第三方来完成，这个第三方机构称为认证中心(Certification Authority，CA)。CA 负责证明所有成员的身份，每个实体(人或设备)都可以通过一定的方式在 CA 中申请证书(certificate)。

目前使用的证书标准为 ITU 制定的 X.5093，许多政府机关和公司在从事 CA 证书的分配和管理工作。对于学校或企业用户来说，也可以在内部网络中创建自己的 CA。例如，Windows Server 2003 等操作系统就提供了 CA 功能。

有关非对称加密系统中密钥管理的详细内容将在本书的第 3 章进行详细介绍。

习　题

2-1　在现代通信中，为什么要使用数据加密技术？

2-2　名称解释：数据加密、对称加密和非对称加密、序列密码和分组密码、软件加密和硬件加密。

2-3　以“恺撒密码”为例，说明简单替换密码在古典密码学应用上的作用。

2-4　什么是“一次一密”密码？举例说明其应用特点。

2-5　以 A5/1 为例，介绍流密码的工作原理。

2-6　介绍 Feistel 密码结构的工作原理。

2-7　联系 Feistel 密码结构，分别介绍 DES、3DES 和 AES 的算法特点。

2-8　与对称加密相比，非对称加密在实现原理和应用上有哪些特点？

2-9　介绍 RSA 算法的工作原理。

2-10　什么是数字签名？在对称加密方式和非对称加密方式中分别是如何实现的？有何特点？

2-11　什么是报文鉴别？Hash 函数在报文鉴别的实现上有何特点？

2-12　介绍报文鉴别的一般实现方法，并分析其报文的原始性和完整性是如何实现的。

2-13　介绍 MD5 算法的工作原理。

2-14　与 MD5 相比，SHA 有何特点？

2-15　在数据加密中，密钥管理有哪些重要性？

2-16　分别介绍对称加密和非对称加密系统中密钥管理的特点和实现方法。

第 3 章 PKI/PMI 技术及应用

随着公钥加密技术在网络安全领域的应用，以提供身份认证、数据完整性和消息保密性等安全服务为核心的公钥基础设施（Public Key Infrastructure，PKI）已成为在网络环境中为各类应用提供安全支撑的重要技术，而基于角色的访问控制（Role Based Access Control，RBAC）技术是在 PKI 基础上发展起来的。授权管理基础设施（Privilege Management Infrastructure，PMI）则为网络环境中的各类应用提供了统一的授权管理和访问控制策略与机制。概括地讲，PKI 证明用户是谁，而 PMI 证明这个用户有什么权限，能干什么，而且 PMI 需要 PKI 为其提供身份认证。本章在第 2 章的基础上，将系统介绍 PKI 和 PMI 的基本概念、功能和应用特点，使读者更加深入地掌握系统安全的相关技术和方法。

3.1 PKI 概述

PKI 是在公开密钥的理论和技术基础上发展起来的安全技术，它是一个为用户提供数据加密、数字签名等安全应用中所需要的密钥和证书的综合基础平台，是信息安全基础设施的一个重要组成部分。

3.1.1 PKI 的概念

公钥基础设施是利用密码学中的公钥概念和加密技术为网上通信提供的符合标准的一整套安全基础平台。PKI 能为各种不同安全需求的用户提供各种不同的网上安全服务所需要的密钥和证书，这些安全服务主要包括身份识别与鉴别（认证）、数据保密性、数据完整性、不可否认性及时间戳服务等，从而达到保证网上传递信息的安全、真实、完整和不可抵赖的目的。利用 PKI 可以方便地建立和维护一个可信的网络应用环境，从而使得人们在这个无法直接相互面对的环境里，能够确认彼此的身份和所交换的信息，能够安全地从事各种活动。

PKI 的技术基础之一是公开密钥体制。因为在公开密钥体制中加密密钥和解密密钥各不相同，信息的发送者利用接收者的公开密钥对信息进行加密，接收者再利用自己的私有密钥进行解密。这种方式既保证了信息的机密性，又能保证信息的不可抵赖性。

PKI 的技术基础之二是加密机制。在 PKI 中，所有在网络中传输的信息都是经过加密处理的。为此，加密算法的可靠性决定了 PKI 系统的可靠性，加密系统的效率决定了 PKI 系统的效率。

因此，从技术上讲，PKI 可以作为支持认证、完整性、机密性和不可否认性的技术基础，从技术上解决网上身份认证、信息完整性和不可抵赖等安全问题，为网络应用提供可靠的安

全保障。然而，PKI绝不只涉及到技术层面的问题，还要涉及到电子政务、电子商务以及国家信息化的基础设施，是相关技术、应用、组织、规范和法律的总和，是一个综合各方面因素的宏观体系。

3.1.2 PKI与网络安全

随着以计算机网络为基础的现代信息技术的发展，电子政务、电子商务等网上电子业务已被人们所接受，并得到不断普及。在网上电子业务的活动中，一方面需要确认双方的合法身份，防止出现虚假身份；另一方面必须保证业务信息的安全性，防止信息被窃取。同时，一旦发生纠纷，必须能够提供充足的证据以供仲裁。所以，要推动电子业务活动的正常运行，就必须从技术上实现身份认证和安全传输，保证服务的权威性、不可否认性和数据的完整性。

在网上电子业务活动中需要确定可依赖的身份，因为仅仅拥有一对公钥和私钥是不足以确立一个可依赖的身份认证的。如果要在计算机网络中创建一个与传统纸上交易等效的环境，还需要一套公钥基础设施的支持，具体要求如下。

（1）安全策略，以规定加密系统在何种规则下运行。

（2）产生、存储和管理密钥的产品。

（3）如何产生、分发、使用密钥和证书的一整套过程。

PKI提供了一个安全框架，使各类构件、应用和策略组合起来为网络环境中的相关活动提供以下的安全功能。

- 保密性。保证信息的私有性。
- 完整性。保证信息没有被篡改。
- 真实性。证明一个人或一个应用的身份。
- 不可否认性。保证信息不能被否认。

在实现方式上，PKI支持SSL、IP over VPN和SPMIME等协议，这使得PKI可以支持Web加密、VPN和安全邮件等应用。而且，PKI支持不同CA间的交叉认证，并能实现证书、密钥对的自动更换。一个完整的PKI产品除主要功能外，还包括交叉认证、支持LDAP协议及支持用于认证的智能卡等功能。基于PKI技术的IPSec协议现在已经成为架构VPN的基础，可以为路由器之间、防火墙之间或者路由器和防火墙之间提供经过加密和认证的通信。另外，安全电子邮件协议（SPMIME）也采用了PKI数字签名技术并支持消息和附件的加密，无须收发双方使用相同的密钥。同时，在网络资源的安全访问、身份认证等系统中，PKI提供了所需的安全支撑。

PKI机制的主要思想是通过公钥证书对某些行为进行授权，其目标是可以根据管理者的安全策略建立起一个分布式的安全体系。PKI的核心是要解决网络环境中的信任问题，确定网络环境中行为主体（包括个人和组织）身份的唯一性、真实性和合法性，保护行为主体合法的安全利益。

作为提供信息安全服务的公共基础设施，PKI已成为世界各国共同采用的最佳的安全体系。在我国，已在金融、政府和电信等部门建立了大量的PKI认证服务中心，在此基础上正在加强系统之间、部门之间以及国家之间PKI体系的互联互通，提供更广泛、更权威的网络安全认证服务。

3.1.3 PKI 的组成

一个典型的 PKI 的组成如图 3-1 所示，其中包括 PKI 安全策略、软硬件系统、认证机构、注册机构、证书发布系统和 PKI 应用等。

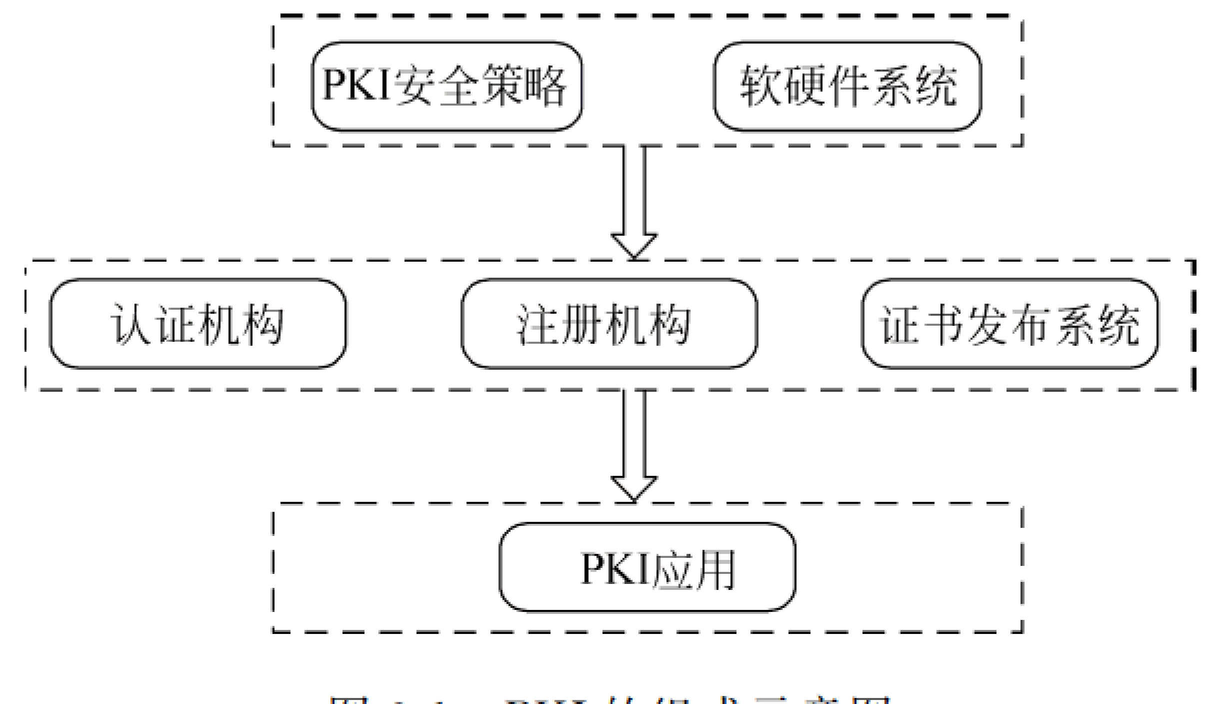


图 3-1　PKI 的组成示意图

1. PKI 安全策略

PKI 安全的策略创建并定义了一个用于实施信息安全的策略，同时也定义了密码系统的使用方法和原则。一般情况下，在 PKI 中有两种类型的策略：一是证书策略，用于管理证书的使用，例如确认某一 CA 是在 Internet 上的公有 CA 还是某一企业内部的私有 CA；另一种是 CPS(Certificate Practice Statement，认证操作管理规范)。一些由商业证书发放机构(CCA)或者可信任的第三方管理的 PKI 系统需要 CPS。PKI 安全策略如下。

(1) CA 的创建和运作方式。

(2) 证书的申请、发行、接收和废除方式。

(3) 密钥的产生、申请、存储和使用方式。

2. 认证机构

认证机构(Certificate Authority，CA)也称为"认证中心"，它是 PKI 的信任基础，它管理公钥的整个生命周期，其作用包括发放证书、规定证书的有效期和通过发布证书废除列表(CRL)，确保必要时可以废除证书。CA 必须是各行业、各部门及公众共同信任的、认可的、权威的、不参与交易的第三方网上身份认证机构。CA 制定了一些规则，这些规则可以使申请和使用证书的用户确信该 CA 是可以依赖的。描述 CA 在各方面受约束的情况及运作方式的规则都被定义在 CPS 中，CPS 最初是由美国律师协会在其数字签名指南(Digital Signature Guidelines)中提出来的。管理证书的 CA 必须将其认证操作管理规范在用户申请证书时以方便用户查阅的方式提供给用户，以便用户查阅，由用户确定是否需要在该 CA 申请数字证书。如果一个 CA 没有 CPS，那么人们就很可能会怀疑该 CA 的真实性，并降低对该 CA 所颁发的数字证书的信任程度。本章随后将会对 CA 进行详细介绍。

3. 注册机构

注册机构(Registered Authority，RA)提供用户和 CA 之间的一个接口，它获取并认证用户的身份，向 CA 提出证书请求。RA 主要完成收集用户信息和确认用户身份的功能。这里指的用户，是指向 CA 申请数字证书的客户，可以是个人、组织或政府机构等。注册管理一般由一个独立的 RA 来承担。它接受用户的注册申请，审查用户的申请资格，并决定是

否同意CA给其签发数字证书。

需要说明的是,RA并不给用户签发证书,而只是对用户进行资格审查。因此,RA可以设置在直接面对客户的业务部门,如银行的营业部、机构认证部门等。当然,对于一个规模较小的PKI应用系统来说,可将注册管理的职能由认证中心CA来完成,而不设立独立运行的RA。但这并不是取消了PKI的注册功能,而只是将其作为CA的一项功能而已。PKI国际标准推荐由一个独立的RA来完成注册管理的任务,以增强应用系统的安全性。

4. 证书发布系统

证书发布系统负责证书的发放。目前一般要求证书发布系统可以Web方式与Internet用户交互,用于处理在线证书业务,方便用户对证书进行申请、下载、查询、注销和恢复等操作。

5. PKI应用

PKI的应用非常广泛,包括在Web服务器和浏览器之间的通信、电子邮件、电子数据交换(Electronic Data Interchange,EDI)、在Internet上的信用卡交易和虚拟专用网(Virtual Private Network,VPN)等。同时,随着以Internet为主的计算机网络的发展,新的PKI的应用也在不断出现和发展。

另外,为了为应用程序提供PKI服务,在PKI系统的组成中还应有PKI应用接口。PKI应用接口是通过PKI的协议标准规范PKI系统各部分之间相互通信的格式和步骤。而API(Application Programming Interfaces,应用程序接口)则定义了如何使用这些协议,并为上层应用提供PKI服务。当应用程序需要使用PKI服务,如获取某一用户的公钥、请求证书撤销信息或请求证书时,将会用到API。目前API没有统一的国际标准,大部分都是操作系统或某一公司产品的扩展,并在其产品应用的框架内提供PKI服务。

一个简单的PKI系统包括CA、RA和相应的PKI存储库。CA用于签发并管理证书;RA可作为CA的一部分,也可以独立,其功能包括个人身份审核、CRL管理、密钥产生和密钥对备份等;PKI存储库包括LDAP(Light Directory Access Protocol,轻型目录访问协议)目录服务器和普通数据库,用于对用户申请信息、证书、密钥、CRL和日志等信息进行存储和管理,并提供一定的查询功能。

3.2 认证机构

PKI系统的关键是如何实现对密钥的安全管理。公开密钥机制涉及公钥和私钥,私钥由用户自己保存,而公钥在一定范围内是公开的,需要通过网络来传输。所以,公开密钥体制的密钥管理主要是对公钥的管理,目前较好的解决方法是采用大家共同信任的认证机构。

3.2.1 CA的概念

认证机构是整个网上电子交易等安全活动的关键环节,主要负责产生、分配并管理所有参与网上安全活动的实体所需的数字证书。在公开密钥体制中,数字证书是一种存储和管理密钥的文件。它是一种采用特定格式的具有权威性的电子文档,其主要作用是证明证书中列出的用户名称与证书中列出的公开密钥相对应,并且所有信息都是合法的。如果要验证其合法性,就必须要有一个可信任的主体对用户的证书进行公证,证明主体的身份及与公

钥之间的对应关系,CA 便是这样的一个管理和能够提供相关证明的机构。

CA 是一个具有权威性、可信赖性和公正的第三方信任机构,专门解决公开密钥机制中公钥的合法性问题。CA 是整个 PKI 系统的核心,负责发放和管理数字证书,其功能类似于办理居民身份证、出入境护照等证书的发证机关。在 PKI 系统中,CA 采用公开密钥机制,专门提供网络身份认证服务,负责签发和管理数字证书。同时,在证书发布后 CA 还负责对证书进行撤销、更新和归档等管理。

由此可见,CA 是保证电子商务、电子政务、网上银行和网上证券等安全交易的权威的、可信任的和公正的第三方机构,是 PKI 系统的核心。

在证书管理的角度来看,每一个 CA 的功能是有限的,需要按照上级策略认证机构制定的策略,负责具体的用户公钥证书的签发、生成和发布,以及 CRL 的生成和发布等职能。CA 的主要职能如下。

(1) 制订并发布本地 CA 策略。但本地 CA 策略只能是对上级 CA 策略的补充,而不能违背。

(2) 对下属各成员进行身份认证和鉴别。

(3) 发布本 CA 的证书,或代替上级 CA 发布证书。

(4) 产生和管理下属成员证书。

(5) 证实 RA 的证书申请,向 RA 返回证书制作的确认信息,或返回已制作好的证书。

(6) 接收和认证对它所签发的证书的撤销申请。

(7) 产生和发布它所签发的证书和 CRL。

(8) 保存证书信息、CRL 信息、审计信息和它所制订的策略。

3.2.2 CA 的组成

一个典型 CA 系统包括安全服务器、注册机构、CA 服务器、LDAP 目录服务器和数据库服务器等,如图 3-2 所示。

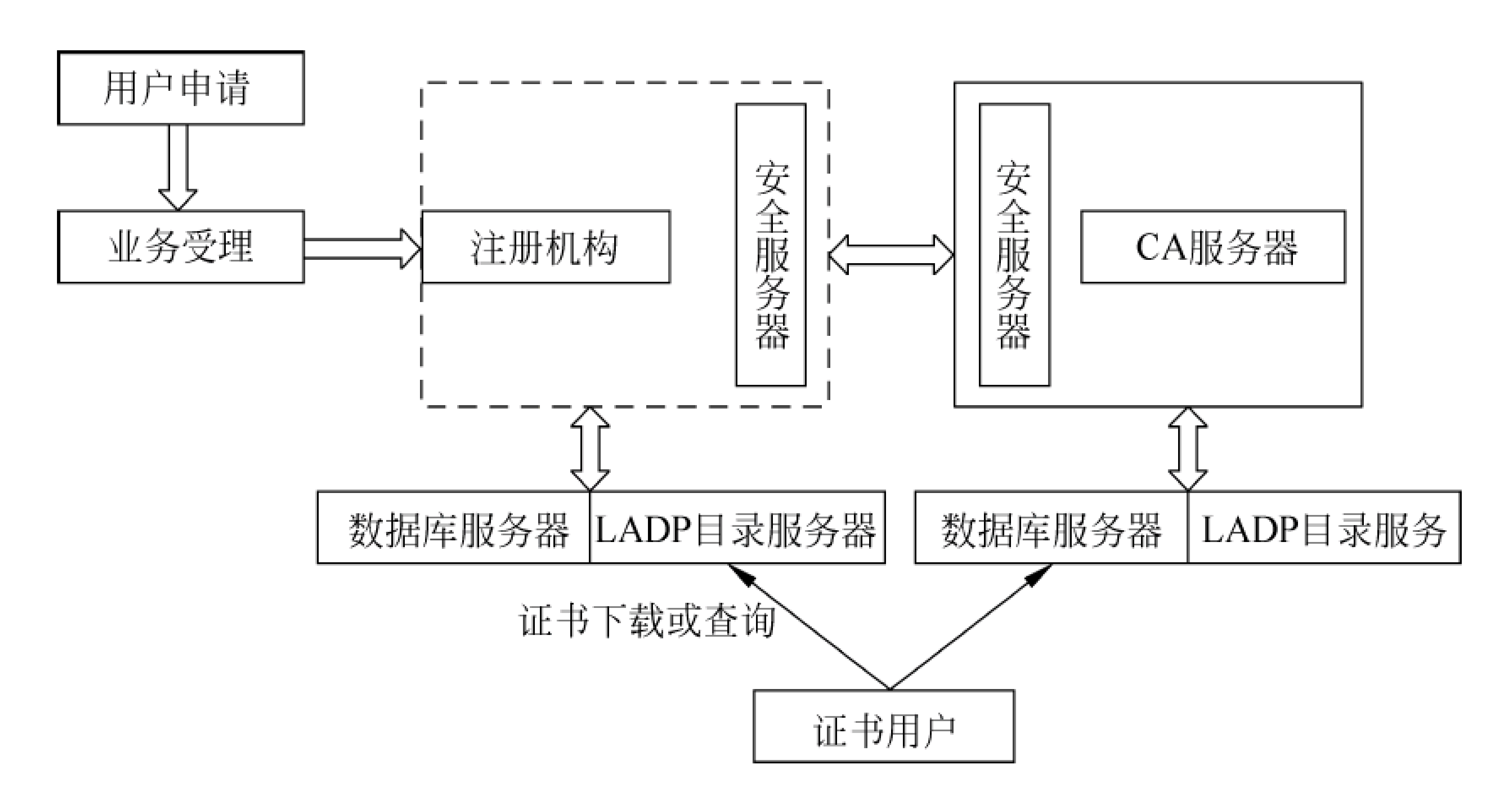


图 3-2 典型 CA 的组成

1. 安全服务器

安全服务器是面向证书用户的提供安全策略管理的服务器,该服务器主要用于提供证书申请、浏览、证书撤销列表及证书下载等安全服务。作为 CA 系统的安全保障,用户与安

全服务器之间的通信一般采取 SSL 加密方式，但不需要对用户进行身份认证。

当 CA 颁发了证书后，该证书首先交给安全服务器。用户一般从安全服务器上获得证书，然后用户与各类服务器之间的所有通信，包括用户填写的申请信息及浏览器生成的公钥均以安全服务器的密钥进行加密传输。只有安全服务器利用自己的私钥解密才能得到明文，这样可以防止其他人通过窃听得到明文。从而保证了证书申请和传输过程中信息的安全性。

2. CA 服务器

CA 服务器是整个认证机构的核心，负责证书的签发。CA 首先产生自身的私钥和公钥（密钥长度至少为 1024 位），然后生成数字证书，并且将数字证书传输给安全服务器。CA 还负责为操作员、安全服务器及注册机构服务器生成数字证书。安全服务器的数字证书和私钥也需要通过安全方式传输给安全服务器。CA 服务器中存储有 CA 的私钥及发行证书的脚本文件，出于安全的考虑，应将 CA 服务器与其他服务器隔离，确保认证机构的安全。

3. 注册机构

注册机构服务器面向注册机构的操作员，在 CA 体系结构中起着承上启下的作用。一方面向 CA 转发安全服务器传输过来的证书申请请求；另一方面向 LDAP 目录服务器和安全服务器转发 CA 颁发的数字证书和证书撤销列表。

4. LDAP 目录服务器

LDAP 目录服务器提供目录浏览服务，负责将注册机构服务器传输过来的用户信息及数字证书加入到服务器上。这样其他用户通过访问 LDAP 目录服务器就能够得到数字证书。

5. 数据库服务器

数据库服务器是认证机构中的关键组成部分，用于认证机构中数据（如密钥和用户信息等）、日志等统计信息的存储和管理。根据数据库技术和网络存储技术的发展，在实际应用中数据库系统应采取多种安全措施（如磁盘阵列、双机备份和分布式处理等），以维护数据库系统的安全性、稳定性、可伸缩性和高效性。

3.2.3 CA 之间的信任关系

认证机构用于创建和发布证书，但一个 CA 一般仅为一个称为安全域（security domain）的有限群体发放证书。每个 CA 只覆盖一定的作用范围，不同的用户群体往往拥有各自不同的 CA。在 X.509 规范中对于信任的定义是：如果实体 A 认为实体 B 会严格地按照 A 对它的期望那样行动，就说 A 信任 B。信任关系是 PKI 系统中的重要组成部分，用来研究用户与 CA 的信任关系以及 CA 间的相互信任关系。

从实际应用来看，不同的组织或单位往往具有自己的 PKI 系统，而这些不同的 PKI 系统之间又需要建立彼此之间的联系。因此，解决单个 PKI 系统中用户与 CA 之间的信任问题，以及各个独立 PKI 系统间的交叉信任问题就显得尤为重要。

1. 单 CA 信任模型

如图 3-3(a)所示，单 CA 信任模型是最基本的信任模型，也是目前许多组织或单位在 Intranet 中普遍使用的一种模型。在这种模型中，整个 PKI 系统只有一个 CA，该 CA 为 PKI 中的所有终端用户签发和管理证书。PKI 中的所有终端用户都信任这个 CA。每个证

书路径都起始于该CA的公钥，该CA的公钥成为PKI系统中唯一的用户信任节点。信任节点也称为“认证起点”或“信任锚”(trust anchor)，它是整个PKI系统中CA的根。

优点：容易实现，易于管理，只需要建立一个根CA，所有的用户都能实现相互认证。

缺点：不易扩展，无法满足不同群体用户的需求。

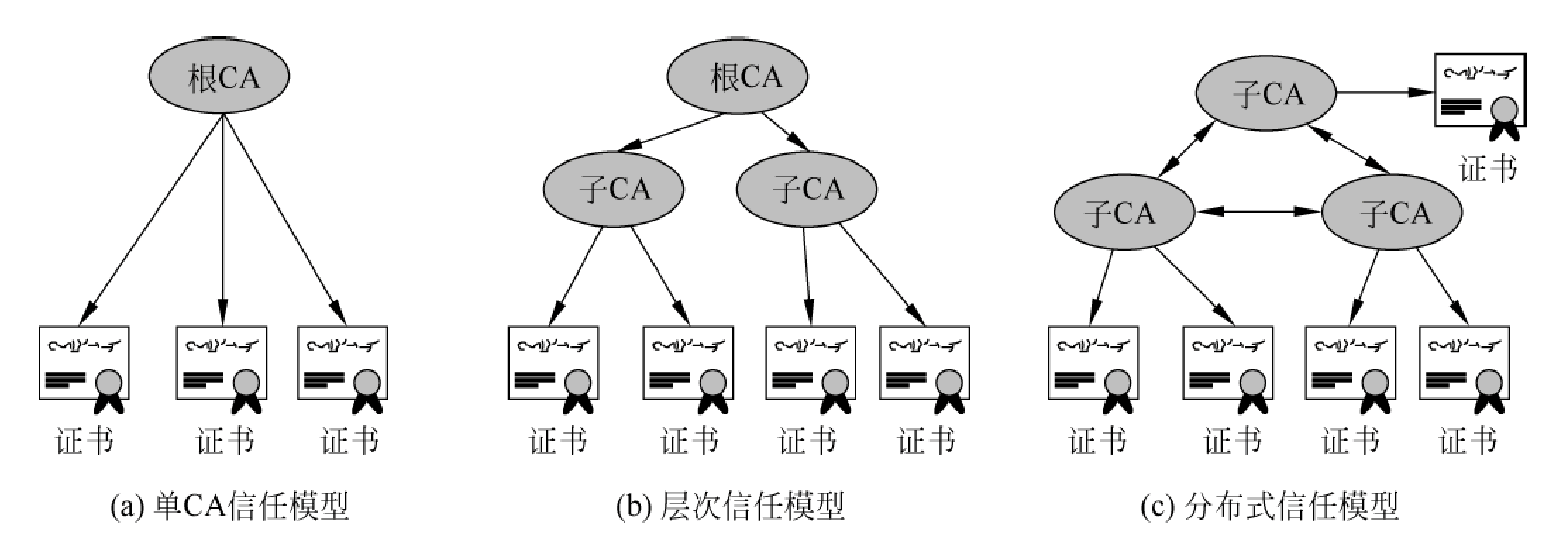


图3-3　单CA、层次和分布式信任模型

2. 层次信任模型

层次信任模型也称为分级信任模型，它是一个以主、从CA关系建立的分级PKI结构，具体结构如图3-3(b)所示。层次信任模型是典型的树型结构，树根为根CA，是整个PKI的信任锚，所有实体都信任它。树枝向下伸展，树叶在末端，代表申请和使用证书的终端用户。

作为信任锚，根CA通常不直接为终端用户颁发证书，而只为子CA颁发证书。在根CA下面可以存在多层子CA，子CA是所在实体集合的根。两个不同的终端用户进行交互时，双方都提供自己的证书和数字签名，通过根CA来对证书进行有效性和真实性的认证。信任关系是单向的，即上级CA可以而且必须认证下级CA，而下级CA不能认证上级CA。

基于层次信任模型的PKI系统由于其简单的结构和单向的信任关系，具有以下的优点。

(1) 增加新的子CA比较容易。新加的子CA可以直接加到根CA下面，也可以加到某个子CA下面。这两种情况都很方便，容易实现。

(2) 证书路径由于其单向性，所以容易扩展，可生成从终端用户证书到信任锚的简单明确的路径。

(3) 证书短小、简单。因为用户可以根据CA在PKI中的位置来确定证书的用途。

层次信任模型也具有如下缺点(整个PKI系统信任单个根CA是导致这些缺点的根源)。

(1) 单个CA的失败会影响整个PKI系统。与根CA的距离越短，则造成的影响越大。另外，由于所有的信任都集中在根CA，一旦根CA出现故障，将导致整个PKI系统瘫痪。

(2) 创建一个所有国家、地区、组织或单位都信任的根CA存在很多困难。

3. 分布式信任模型

分布式信任模型也称为网状信任模型，在这种模型中CA间存在着交叉认证，如图3-3(c)所示。如果任何两个CA间都存在着交叉认证，则这种模型就成为严格的网状信任模型。与在PKI系统中的所有实体都信任唯一根CA的层次信任模型相反，网状信任模型把信任分散到两个或更多个CA上。分布式信任模型的优点如下。

（1）具有更好的灵活性。因为存在多个信任锚，所以单个 CA 安全性的削弱不会影响到整个 PKI 系统。

（2）增加新的 CA 更为容易。当一个组织想要整合各个独立开发的 PKI 系统时，这种信任方式是很有效的。

（3）系统的安全性较高。

分布式信任模型的主要缺点是路径发现比较困难。从终端用户证书到信任锚建立证书的路径是不确定的，因为存在多种选择，使得路径发现比较困难。

4. 桥 CA 信任模型

桥 CA 信任模型也称为中心辐射式信任模型，它是为克服层次信任模型和分布式信任模型的缺点而设计的，它可连接不同的 PKI 系统，如图 3-4 所示。

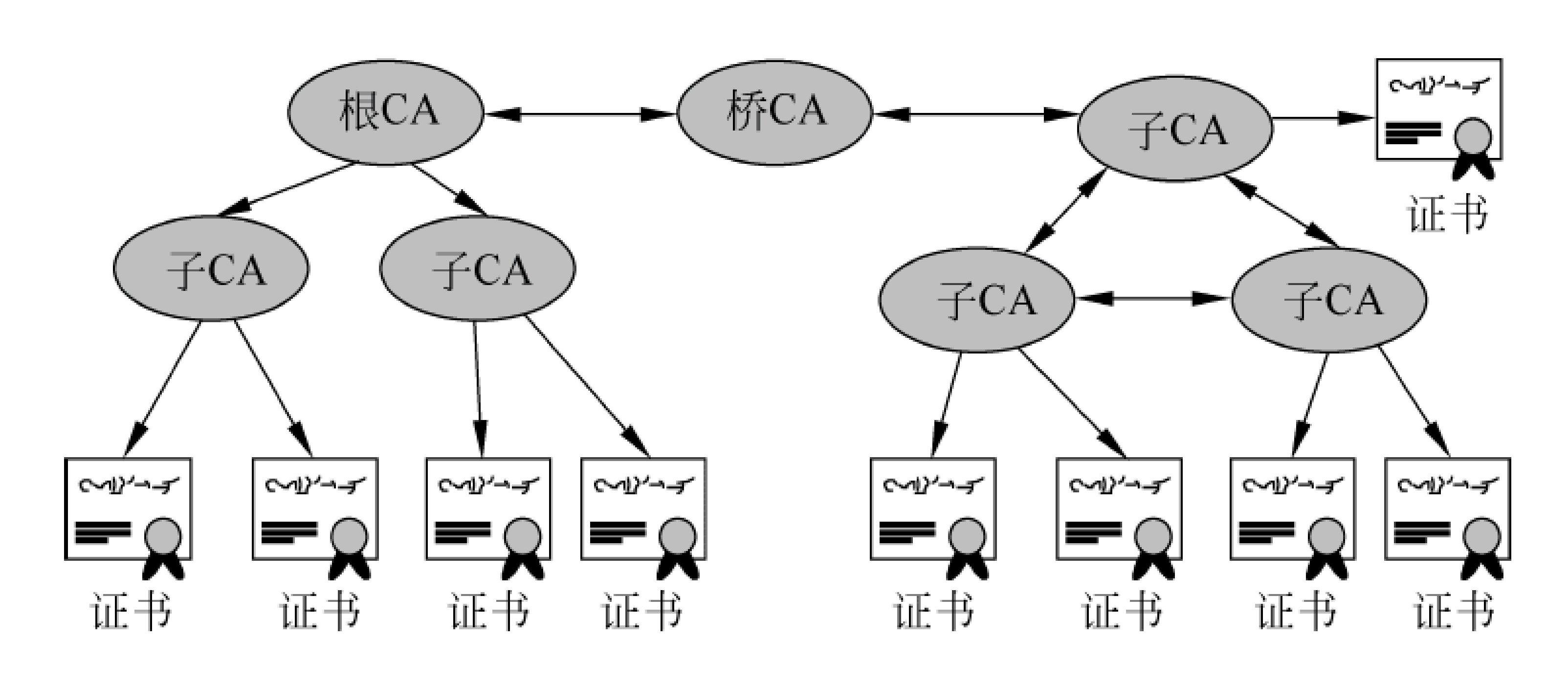


图 3-4　桥 CA 信任模型

不同于分布式信任模型中的 CA，桥 CA 与不同的信任域（子 CA）建立对等的信任关系，允许用户保持原有的信任锚。这些关系被结合起来形成信任桥，使得来自不同信任域的用户通过桥 CA 相互作用。其中，桥 CA 不是一个树形结构的 CA，也不像分布式信任模型中的 CA，它不直接向用户颁发证书。桥 CA 只是一个单独的 CA 而非信任锚，根 CA 是一个信任锚。桥 CA 与不同的信任域之间建立对等的信任关系，允许用户保留他们自己的原始信任锚。

正如在网络中所使用的 Hub 一样，任何结构类型的 PKI 都可以通过桥 CA 连接在一起，实现彼此之间的信任，每一个单独的信任域都可以通过桥 CA 扩展到整个 PKI 系统中。桥 CA 模型的优点如下。

（1）实用性强。该模型非常符合目前证书管理机构的特点。

（2）证书路径较易发现，路径较短。桥 CA 架构的 PKI 比起具有相同数量 CA 分布式信任模型的 PKI 系统，具有更短的可信任路径。

桥 CA 的缺点如下。

（1）证书路径的有效发现和确认仍然不很理想。因为基于桥 CA 模型的 PKI 系统可能会包括部分分布式信任模型。

（2）大型 PKI 目录的互操作性仍不方便。

（3）证书复杂。在基于桥 CA 信任模型的 PKI 系统中，桥 CA 需要利用证书信息来限制不同 PKI 的信任关系，这会导致证书的处理更为复杂。

（4）证书和证书状态信息不易获取。

5. Web 信任模型

Web 信任模型构建在 Web 浏览器的基础上，浏览器厂商在浏览器（如 Internet Explorer、Tencent Traveler、Mozilla Firefox 和 Opera 等）中内置了多个根 CA，每个根 CA 相互间是平行的，浏览器用户同时信任多个根 CA 并把这些根 CA 作为自己的信任锚。以 Internet Explorer 为例，选择"工具"→"Internet 选项"→"内容"→"证书"命令，在打开的如图 3-5 所示的"证书"对话框中就会看到 Internet Explorer 的信任锚。



图 3-5　Internet Explorer 的信任锚

Web 信任模型表面上看与分布式信任模型非常相似，实际上它更接近层次信任模型。Web 信任模型通过与相关域进行互连而不是扩大现有的主体群，来使用户实体成为在浏览器中所给出的所有域的依托方，如图 3-6 所示。各个嵌入的根 CA（如图 3-5 所示）直接内置在各个浏览器软件中，使用中这些根 CA 不会显示有关信息。由于各个根 CA 是浏览器厂商内置的，浏览器厂商隐含认证了这些根 CA，这样浏览器厂商就成为事实上隐含的根 CA。

Web 信任模型的优点为：方便简单，操作性强，对终端用户的要求较低。用户只需简单的信任嵌入的各个根 CA 即可，尤其适合于目前在 Internet 和 Intranet 中的应用。

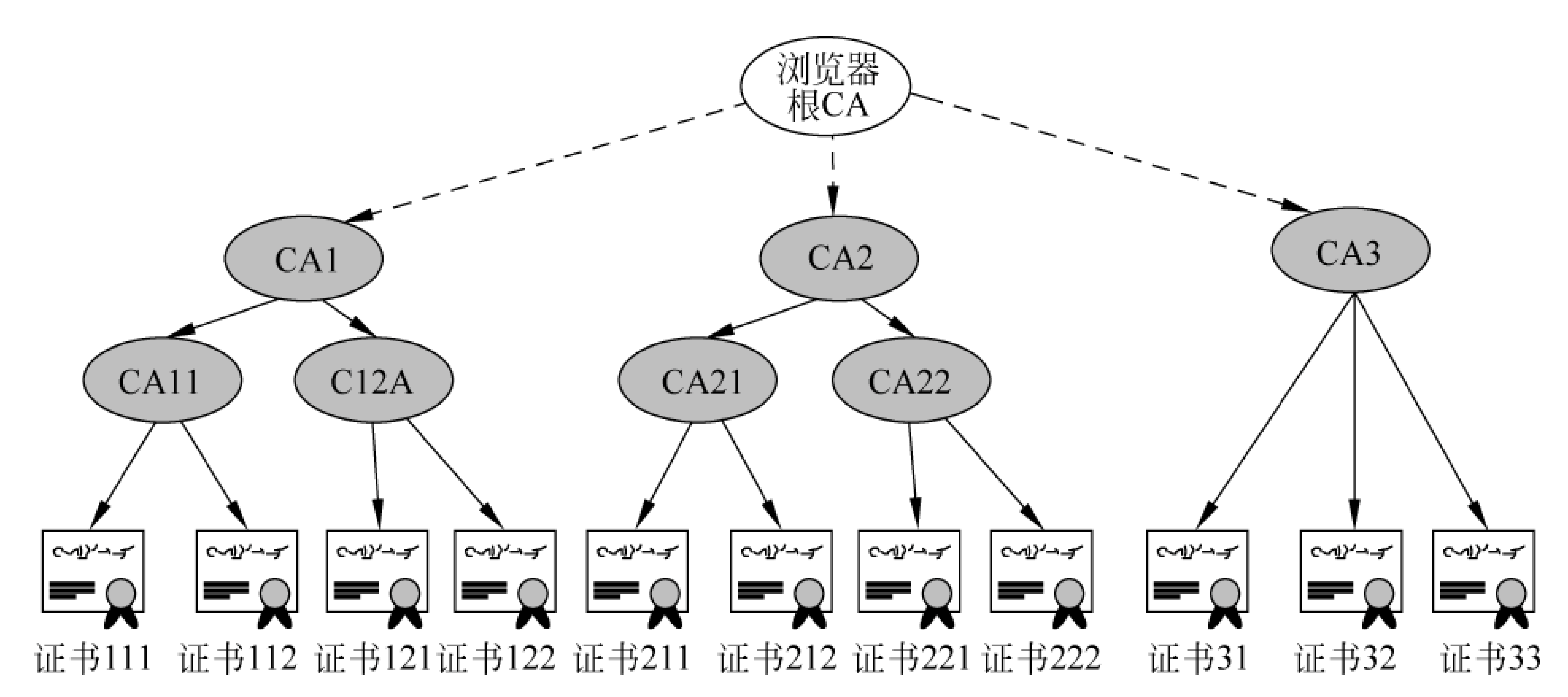


图 3-6　Web 信任模型

Web 信任模型的缺点如下。

(1) 安全性较差。如果这些根 CA 中有一个存在安全问题,即使其他根 CA 仍然值得用户信赖,安全性也将被破坏。目前还没有有效可行的机制来撤销嵌入到浏览器中的根 CA(即密钥)。用户也难于查出到底哪一个根 CA 存在安全问题,这一切都依赖于浏览器厂商。

(2) 根 CA 与终端用户信任关系模糊。终端用户与嵌入的根 CA 间交互十分困难。终端用户可在不同的站点得到不同的浏览器,他很难知道某个浏览器中嵌入了哪些根 CA,并且用户一般不可能对证书颁发有足够的了解以至于与 CA 直接接触。同样,嵌入的根 CA 也无法知道和确定它的依托方是谁。

(3) 根 CA 预先安装,难以扩展。

6. 以用户为中心的信任模型

在以用户为中心的信任模型中,每个用户都直接决定信赖哪个证书和拒绝哪个证书。没有可信的第三方作为 CA,终端用户就是自己的根 CA,如图 3-7 所示。

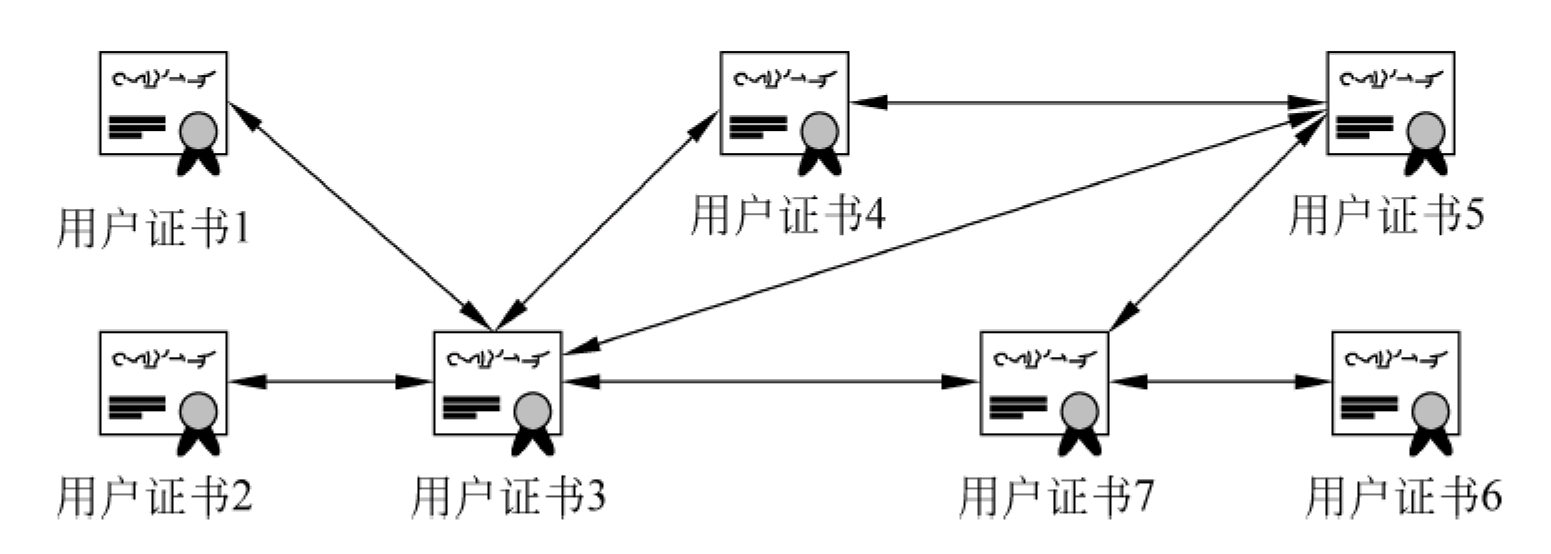


图 3-7 以用户为中心的信任模型

以用户为中心的信任模型的优点如下。

(1) 安全性很强。

(2) 用户可控性很强。用户可自己决定是否信赖某个证书。也就是说,每个用户可以直接和独立地决定信赖哪个证书和拒绝哪个证书。

以用户为中心的信任模型的缺点如下。

(1) 使用范围较窄。由于普通用户很少关心安全方面的问题,也缺乏相应的安全知识,将发放和管理证书的任务交给用户在许多应用中是不现实的。

(2) 这种信任模型在某些企业、金融机构或者政府机关的网络环境中是不适用的。因为在这些群体中,往往需要以组织的方式控制一些公钥,而不希望完全由用户自己控制。

表 3-1 对前面介绍的各种 CA 信任模型的特点进行了描述。

表 3-1 各种 CA 信任模型的性能说明

信任模型	实用性	方便性	可扩展性	安全性	高效性	灵活性	互操作性	应用范围
单 CA	低	高	高	高	高	低	低	窄
层次	中	高	高	高	高	低	高	窄
分布式	中	低	低	高	低	高	高	广
桥 CA	高	低	高	高	低	高	高	广
Web	低	高	低	低	高	低	低	窄
以用户为中心	中	低	低	高	低	低	高	窄

3.2.4 密钥管理

密钥管理也是PKI系统(主要指CA)中的一个核心问题。密钥管理主要是指密钥对的安全管理,包括密钥产生、密钥备份、密钥恢复和密钥更新等。

1. 密钥产生

密钥对的产生是证书申请过程中重要的一步,其中产生的私钥由用户保留,公钥和其他信息则交由CA中心进行签名,从而产生证书。根据证书类型和应用的不同,密钥对的产生也有不同的形式和方法。对于普通用户证书,一般由浏览器或固定的终端应用程序产生,这样产生的密钥强度较小,不适用于安全要求较高的领域。而对于比较重要的证书,如机构证书(CA证书、RA证书)等,密钥对一般由专用应用程序或CA中心直接产生,这样产生的密钥强度大,适合于重要的应用场合。

另外,根据密钥对应用场合的不同,也可能会有不同的产生方式。例如签名密钥可能在客户端或RA中心产生,而加密密钥则需要在CA中心直接产生。

2. 密钥备份和恢复

在一个PKI系统中,对密钥对的安全管理非常重要,其中备份是最常用到的一种方式。如果没有安全保障,当密钥丢失后,将意味着使用该密钥加密的数据无法打开,对于一些重要数据,这将是灾难性的事故。所以,密钥的备份和恢复也是PKI系统中非常重要的一个安全环节。在部署和使用PKI系统时,PKI系统的提供者必须确保即使密钥丢失,受密钥加密保护的重要信息也能够恢复。

企业级的PKI系统至少应该提供对加密的安全密钥的存储、备份和恢复。密钥一般用口令进行保护,而口令丢失则是管理员最常见的安全疏漏之一。所以,PKI系统应该能够备份密钥,即使口令丢失,它也能够让用户在一定条件下恢复该密钥,并设置新的口令。

另外,使用PKI系统的企业也应该考虑所使用密钥的生命周期,它包括密钥和证书的有效时间,以及已撤销密钥和证书的归档等。

3. 密钥更新

对每一个由CA颁发的证书都会存在有效期,密钥对生命周期的长短由签发证书的CA中心来确定,每一个CA系统所颁发的证书的有效期限有所不同,一般为2~3年。当用户的私钥被泄漏或证书的有效期快到时,用户应该更新私钥。

3.3 证书及管理

PKI采用证书管理公钥,通过第三方的可信任机构CA把用户的公钥和用户的其他标识信息捆绑在一起,在Internet或Intranet上验证用户的身份。数字证书的管理方式在PKI系统中起着关键作用。

3.3.1 证书的概念

数字证书也称为数字标识(Digital Certificate,或Digital ID)。它提供了一种在Internet等公共网络中进行身份验证的方式,用来标识和证明网络通信双方身份的数字信

息文件，其功能与驾驶员的驾照或日常生活中的身份证相似。数字证书由一个权威的证书认证机构发行，在网络中可以通过从CA中获得的数字证书来识别对方的身份。在网上进行电子商务活动时，交易双方需要使用数字证书来表明自己的身份，并使用数字证书来进行有关交易操作。例如，在进行网上银行的相关操作时，必须安装与银行账号相对应的数字证书，否则系统是无法完成相关操作的。目前，像银行等单位为用户提供的数字证书文件既可以安装在用户的计算机中，也可以保存在U盘等存储介质中。例如，在现在的公安专网中，每一个民警都有一个用于标识自己身份的U盘，在该U盘中保存了民警自己的数字证书，每个民警访问网络的权限都集中在该数字证书中。通俗地讲，数字证书就是个人或单位在Internet等公共网络上的身份证。

比较专业的数字证书定义是：数字证书是一个经证书授权中心数字签名的包含公开密钥拥有者信息及公开密钥的文件。最简单的证书包含一个公开密钥、名称及证书授权中心的数字签名。一般情况下，证书中还包括密钥的有效时间、发证机关(证书授权中心)的名称及该证书的序列号等信息，证书的格式遵循相关国际标准。

通过数字证书就可以使信息传输的保密性、数据交换的完整性、发送信息的不可否认性及交易者身份的确定性这四大网络安全要素得到保障。

3.3.2 数字证书的格式

在Internet和Intranet中，应用程序使用的证书都来自不同的厂商或组织，为了实现可交互性，要求证书能够被不同的系统识别，符合一定的格式，并实现标准化。目前有X.509、WTLS(Wireless Transport Layer Security，无线传输层安全)和PGP(Pretty Good Privacy。一种采用公钥加密体系的电子邮件加密软件。)等多种数字证书，但应用最为广泛的是X.509，X.509为数字证书及其CRL格式提供了一个标准。

需要说明的是，X.509本身不是Internet标准，而是ITU(国际电信联盟)的标准，它定义了一个开放的框架，并在一定范围内可以进行扩展。为了提供公用网络用户目录信息服务，ITU于1988年制定了X.500系列标准。其中X.500和X.509是安全认证系统的核心。X.500定义了一种区别命名规则，以类似互联网中DNS的命令树来确保用户名称的唯一性；而X.509则为X.500用户名称提供了通信实体鉴别机制，并规定了实体鉴别过程中广泛适用的证书语法和数据接口，X.509称为证书。

X.509目前有4个版本：X.509 v1、v2、v3和v4。其中，X.509 v1提供了基于X.509公钥证书的目录访问认证协议。1993年ITU公布了X.509 v2，其中增强了对目录访问控制和鉴别的支持。证书由用户公开密钥和用户标识符组成。此外还包括版本号、证书序列号、CA标识符、签名算法标识、签发者名称和证书有效期等信息。还定义了包含扩展信息的数字证书，该版数字证书提供了一个扩展信息字段，用来提供更多的灵活性及特殊应用环境下所需的信息传送。1997年，ISO/IEC(IEC即“International Electrotechnical Commission，国际电工委员会”，1947年当ISO成立时IEC并入ISO，从1976年开始，ISO和IEC成为法律上独立的两个组织。其中，IEC负责有关电工、电子领域的国际标准化工作，其他领域由ISO负责。)和ANSI X9开发了X.509 v3，它是基于公开密钥证书的目录鉴别协议。v3定义的公开密钥证书协议比v2证书协议增加了14项预留扩展域，例如发证者或证书用户的身份标识、密钥标识、用户或公钥属性、策略(policy)扩展等，同时v3对CRL结构也进行了扩展。X.509 v4(X.509-2000)于2000年推出，v4在扩展了v3的同时，利用属性证书定义了PMI(Privilege Management Infrastructure，特权管理基础设施)模型，即如何利用PKI-CA对用户访问进行授权管理。X.509证书的通用格式如

证书版本号
证书序列号
签名算法标识符
颁发机构名
有效期
实体名称
证书持有者的公开密钥信息
颁发者唯一标识符
证书持有者唯一标识符
签名值

图 3-8　X. 509 数字证书的基本格式

图 3-8 所示，每一个组成域的功能描述如下。

(1) 证书版本号(Version)。指明 X. 509 证书的格式版本。0 表示 X. 509 v1 标准，1 表示 X. 509 v2 标准，依此类推。目前最新的版本为 X. 509 v4。

(2) 证书序列号(Serial Number)。指定由 CA 分配给证书的唯一数字型标识符。当证书被取消时，实际上是将此证书的序列号放入由 CA 签发的 CRL 中，这也是序列号唯一的原因。

(3) 签名算法标识符(Signature)。用来指定由 CA 签发证书时所使用的签名算法。算法标识符用来指定 CA 签发证书时所使用的公开密钥算法和 Hash 算法，须向国际知名标准组织(如 ISO)注册。

(4) 颁发机构名(Issuer)。此域用来标识签发证书的 CA 的 X. 500 DN 名字。包括国家、省市、地区、组织机构、单位部门和通用名。其中，DN(Distinguished Name)是类似于 DNS 名称服务方式，在 LDAP 中目录记录的标识名称为 DN，用来读取某个条目。

(5) 有效期(Validity)。指定证书的有效期，包括证书开始生效的日期和时间，以及失效的日期和时间。每次使用证书时，需要检查证书是否在有效期内。

(6) 实体名称(Subject)。指定证书持有者的 X. 500 唯一名字。包括国家、省市、地区、组织机构、单位部门和通用名，还可包含 E-mail 地址等个人信息。

(7) 证书持有者的公开密钥信息(Subject Public Key Info)。证书持有者公开密钥信息域包含两个重要信息：证书持有者的公开密钥的值和公开密钥使用的算法标识符。此标识符包含公开密钥算法和 Hash 算法。

(8) 颁发者唯一标识符(Issuer Unique Identifier)。该域在 v2 中开始加入。当同一个 X. 500 名字用于多个认证机构时，用一位字符串来唯一标识颁发者的 X. 500 名字。该域为一个可选项。

(9) 证书持有者唯一标识符(Subject Unique Identifier)。该域在 v2 中开始加入。当同一个 X. 500 名字用于多个证书持有者时，用一位字符串来唯一标识证书持有者的 X. 500 名字。该域为一个可选项。

(10) 签名值(Issuer's Signature)。证书颁发机构对证书上述内容的签名值。

3.3.3　证书申请和发放

证书的申请一般有两种方式：在线申请和离线申请。其中，在线申请就是用户登录认证机构的相关网站下载申请表格，然后按要求填写内容。或通过浏览器、电子邮件等在线方式来申请证书，这种方式一般用于申请普通用户证书。离线方式一般通过人工的方式直接到认证机构证书受理点办理证书申请手续，通过审核后获取证书，这种方式一般用于比较重要的场合，如网上银行的在线支付证书等。下面主要以在线申请方式为例进行介绍，申请的步骤如下。

(1) 用户申请。用户使用浏览器通过 Internet 或 Intranet 访问安全服务器，下载 CA 的数字证书，该证书称为根证书。然后在证书的申请过程中使用 SSL 安全方式与服务器建立连接，用户填写个人信息，浏览器生成私钥和公钥对，将私钥保存在客户端的特定文件中，并

且要求用口令保护私钥，同时将公钥和个人信息提交给安全服务器。安全服务器将用户的申请信息传送给注册机构服务器。

（2）注册机构审核。用户与注册机构人员联系，证明自己身份的真实性，或者请求代理人与注册机构联系。注册机构操作员利用自己的浏览器与注册机构服务器建立 SSL 安全通信，该服务器需要对操作员进行严格的身份认证，包括操作员的数字证书、IP 地址等。操作员首先查看目前系统中的申请人员，从列表中找出相应的用户，单击用户名，核对用户信息，并且可以进行适当的修改。如果操作人员同意用户的申请证书请求，必须对证书申请信息进行数字签名。操作员也有权利拒绝用户的申请。操作员与服务器之间的所有通信都采用加密和签名方式，具有安全性、抗抵赖性，保证了系统的安全性和有效性。

（3）CA 发放证书。注册机构向 CA 传输用户的证书申请与操作员的数字签名，CA 操作员查看用户的详细信息，并且验证注册机构操作员的数字签名，如果签名验证通过，则同意用户的证书请求，发放该证书。然后 CA 将证书输出。如果 CA 操作员发现签名不正确，则拒绝证书申请。CA 发放的数字证书中包含以下主要内容。

① 实体（公开密钥拥有者，如人或设备）的身份，包括名称、序列号、IP 地址和单位的名称等，以及其他用以识别单个用户或网络设备（如主机、交换机、防火墙和路由器等）的信息。

② 该实体的公开密钥。

③ 签发该证书的 CA 的数字签名和身份。

④ 证书的有效期。

⑤ 证书的级别（证书可以分为多种级别，较高的级别需要注册者提供更详细的身份证明）。

⑥ 证书 ID 号。

（4）注册机构证书转发。注册机构操作员从 CA 服务器得到新的证书，首先将证书输出到 LDAP 目录服务器以提供目录浏览服务，然后操作员向用户发送一封电子邮件，通知用户证书已经发布成功，并且把用户的证书序列号告诉用户，要求用户到指定的站点下载自己的数字证书。同时，在电子邮件中会告诉用户如何使用安全服务器上的 LDAP 配置，让用户修改浏览器的客户端配置文件以便访问 LDAP 服务器、获得他人的数字证书等。

（5）用户获取证书。一般情况下，利用在线方式申请证书后，用户需要使用证书申请时计算机上的浏览器到指定的站点下载由注册机构转发的证书。期间，需要输入用户的证书序列号。服务器要求用户必须使用申请证书时的浏览器，因为浏览器需要用该证书相应的私钥去验证数字证书。只有保存了相应私钥的浏览器才能成功下载用户的数字证书。

这时用户打开浏览器的安全属性（如图 3-5 所示），就可以发现自己已经拥有了 CA 颁发的数字证书。然后，可以利用该数字证书与其他人或拥有相同 CA 颁发的证书的应用系统使用加密、数字签名方式进行安全通信。

3.3.4 证书撤销

在证书的有效期内，由于私钥丢失或证书持有者解除了与某一组织或单位的关系，该用户所使用的数字证书需要撤销。证书的撤销操作由 CA 完成，当 CA 接收到用户撤销证书的申请时，立即执行证书撤销操作，同时通知用户证书的撤销情况。其实，出于安全考虑，在证书的正常使用中，当用户每次使用证书时系统都要检查用户的证书是否合法和有效。

证书的撤销一般可通过两种方式实现：一种是利用周期性发布机制，主要有证书撤销列表(Certificate Revocation Lists，CRL)；另一种是利用在线查询机制，如在线证书状态协议(Online Certificate Status Protocol，OCSP)。以下分别进行介绍。

1. 利用 CRL 撤销证书

证书撤销列表(又称证书黑名单)为应用程序和其他系统提供了一种检验证书有效性的方式。任何一个证书撤销以后，认证机构会通过发布 CRL 的方式来通知各个相关方。X.509 中 CRL 所包含的主要内容格式如下(结构如图 3-9 所示)。

证书版本号
签名算法
证书签发机构名
本次签发时间
下次签发时间
用户公钥信息
签名算法
签名值

图 3-9　证书撤销列表

(1) 证书版本号。CRL 的版本号，0 表示 X.509 v1 标准，1 表示 X.509 v2 标准，依此类推。目前最新的版本为 X.509 v4。

(2) 签名算法。包含算法标识和算法参数，用于指定证书签发机构用来对 CRL 内容进行签名的算法。

(3) 证书签发机构名。签发机构的 DN 名，由国家、省市、地区、组织机构、单位部门和通用名等组成。

(4) 本次签发时间。本次 CRL 签发时间，遵循 ITU-T X.509 v2 标准的 CA，在 2049 年之前把这个域编码为 UTCTime 类型，在 2050 或 2050 年之后把这个域编码为 GeneralizedTime 类型。

(5) 下次签发时间。下次 CRL 签发时间，遵循 ITU-T X.509 v2 标准的 CA，在 2049 年之前把这个域编码为 UTCTime 类型，在 2050 或 2050 年之后把这个域编码为 GeneralizedTime 类型。

(6) 用户公钥信息。其中包括撤销的证书序列号和证书撤销时间。撤销的证书序列号是指要撤销的由同一个 CA 签发的证书的一个唯一标识号，同一机构签发的证书不会有相同的序列号。

(7) 签名算法。对 CRL 内容进行签名的签名算法。

(8) 签名值。证书签发机构对 CRL 内容的签名值。

另外，CRL 中还包含扩展域和条目扩展域。CRL 扩展域用于提供与 CRL 有关的额外信息，允许团体和组织定义私有的 CRL 扩展域来传送他们独有的信息；CRL 条目扩展域则提供与 CRL 条目有关的额外信息，允许团体和组织定义私有的 CRL 条目扩展域来传送他们独有的信息。

基于 CRL 的周期发布证书状态信息机制，主要有以下优点。

(1) 证书撤销列表的安全性是通过 CA 中心(或者 CA 授权的机构)签名来保证的，所以证书存储的地址并没有受到严格的控制，这样就可以根据需要在适当的地方存储需要的 CRL。

(2) 在 CRL 中，包含一个本列表的颁发日期，以及下一次 CRL 的颁发时间。这两个属性可以帮助管理 CRL 缓冲区。如果证书的撤销频率不是很高，CRL 将会是一个有效的、有较好伸缩性的证书状态信息分发机制。

(3) 使用增量 CRL 机制，仅发布那些自某个基本 CRL 颁发以来新撤销的证书，这样减少了单个签名的信息量，同时增加了 CRL 的实时性并且提高了证书状态响应器(服务器)的应答时间。

在 PKI 系统中，CRL 是自动完成的，而且对用户是透明的。CRL 中并不存放撤销证书

的全部内容，只存放证书的序列号，以便提高检索速率。CRL 产生的主要步骤如下。

（1）RA 建立与 CA 的连接，提出撤销申请。该申请中包括撤销证书的序列号及撤销理由。

（2）CA 将撤销证书的序列号签发到 CRL 中。

（3）系统通过数据库或 LDAP 目录等方式发放新的 CRL，并且提供用户在线查询。

2. 利用 OCSP 撤销证书

尽管利用 CRL 撤销证书具有许多优点，但该方式本身固有的 CRL 的存储位置分散、CRL 的更新无法准确统计及客户端程序比较复杂等缺点，致使基于 CRL 的证书撤销机制在实际应用中存在不足。

在线证书状态协议（OCSP）是 IETF 工作组颁布的用于检查数字证书在当前时刻是否有效的标准协议。该协议提供给用户一条便捷的证书状态查询通道，使 PKI 体系能够更有效、更安全地应用于各个领域。OCSP 可以作为周期性 CRL 的一种替代机制或者补充机制，它对于获得一个证书撤销状态的及时信息是必要的。与 CRL 相比，OCSP 对获得证书撤销信息的及时性要强，所以 OCSP 一般用于网上银行、网上证券和电子政务中的某些关键部门。

OCSP 协议是用于 OCSP 请求者（客户端）和 OCSP 响应器（服务器）之间的一个请求/响应协议。客户端生成一个 OCSP 请求，它包含一个或者多个待查询证书的标识符，客户端可以选择性地对该请求进行数字签名。然后，客户端将请求发送给服务器。OCSP 响应器对收到的请求返回一个响应（出错信息或是确定的回复）。OCSP 响应器返回出错信息时，该响应不用签名。出错信息包括请求编码格式不正确、内部错误、稍后再试、请求需要签名和未授权等内容。OCSP 响应器返回确定的回复时，该响应必须进行数字签名。

OCSP 是一种相对简单的请求/响应协议，它使得客户端应用程序可以测定所需验证的证书状态。协议对 OCSP 客户端和 OCSP 响应器之间需要交换的数据进行了描述。一个 OCSP 请求包含协议版本、服务请求、目标证书标识和可选的扩展项等数据。一个确定的响应由版本号、响应器名称、对每一张被请求证书的回复、可选扩展项、签名算法、对象标识和签名等组成。

OCSP 机制的主要优点。

（1）从 OCSP 响应器得到的信息总是能够反映该证书的真实状态。

（2）与 CRL 相比，每一次证书查询需要处理的信息量要小得多，因为用户只关心当前查询的证书状态，而且客户端应用程序需要处理的返回信息也要少一些。尽管 OCSP 有许多优点，但基于证书响应状态协议的机制也存在一些问题与不确定性。

（1）证书状态响应器应该是一个可信的在线服务器，并为每一个请求提供及时的响应。而且，证书状态响应服务器不能完全替代 CRL 存储库，一定条件下仍然需要访问 CRL 存储库去查找证书。

（2）证书状态响应器难以实现镜像，也难以备份，可能成为通信中的瓶颈。而且，在线响应系统的访问流量可能非常不均匀，使得服务器系统经常处于不稳定的状态，这样很容易受到拒绝服务等攻击。

（3）证书状态的响应服务器必须生成大量的签名，来保证每次响应的真实性和有效性，同时也可能需要验证大量的签名，这些过程将降低服务器的性能，甚至可能出现由于请求等待时间过长而丢失请求信息。

3.3.5 证书更新

在 PKI 系统中,每一份数字证书被颁发以后都有其生命周期。当证书超出了其有效期就被作废而要求更新。进行证书更新的主要原因如下：一是与证书相关的密钥可能达到它有效的生命终点；二是证书即将到期；三是证书中的一些属性发生了变化,必须进行改变。在这些情况下,必须颁发一个新的证书,这称为证书更新或重新证明。根据证书应用对象的不同,证书更新分为普通用户证书更新和机构证书更新两种类型。

1. 普通用户证书更新

普通用户证书一般是指由普通用户根据个人(包括组织或单位)需要所申请和使用的数字证书。普通用户证书更新一般有以下两种方式。

(1) 人工更新。用户向注册机构提出更新证书的申请,RA 根据用户申请信息更新用户的证书。

(2) 自动密钥更新。PKI 系统采用对管理员和用户透明的方式,对快要过期的证书进行自动更新,生成新的密钥对。

2. 机构证书更新

机构证书也是一种证书,只是这种证书专门用来证实机构(如 CA、RA 等)的真实性、合法性、可靠性以及可信任性。机构证书与普通用户证书一样,如果在有效期快到期时,就要进行更新并将更新消息告知所有的相关用户及机构。因此,这就需要一套完整的机制来保证机构证书的顺利更新,从而保证整个系统的有效性和安全性。在一个 PKI 系统中,机构的类型分为各级 CA 机构及 RA 机构,因而机构证书的类型也相应地分为 RA 机构证书和 CA 机构证书。

当机构证书快到期时,就需要对它进行更新操作。它的更新操作与一般普通用户证书有很大的差别。普通用户证书在更新时,只需要向签发机构发出申请,由签发机构撤销旧的证书,并重新产生新的公私密钥对和颁发新的证书,用户证书就更新结束。相比之下,机构证书的更新就复杂得多,它分为根 CA 的更新和下级 CA 的更新。

为了保证系统的连续性,在机构证书更新期间,根 CA 就有多个证书存在。如下所示,根 CA 在更新期间,共有 3 类证书存在(其中 old 表示旧证书,new 表示新证书)。

- oldwithnew。用新证书签发的旧证书。
- newwithold。用旧证书签发的新证书。
- newwithnew。根 CA 自签发的新证书。

其中,oldwithnew 和 newwithold 证书是为了在证书更新期间保持证书认证的连续性,它们在根 CA 证书更新结束时要被全部撤销。oldwithnew 用于旧的用户证书的认证及新旧用户证书的相互认证；newwithold 用于新旧证书的相互认证；newwithnew 用于新证书的认证和颁发新的下级证书。同时在根 CA 更新的同时,也需要用 newwithnew 对证书撤销列表进行操作,并生成新的证书链文件。

下级机构证书的撤销相对根 CA 而言就要简单一些。下级机构证书快到期时,由下级机构向上级 CA 申请证书更新,上级 CA 通过为下级机构颁发新的证书并同时撤销旧的证书来达到下级机构证书的更新目的。但是,下级机构证书更新后,如果是 CA 机构,则要同时重签证书撤销列表并发布到证书目录服务器上,以供用户使用及认证使用。

需要说明的是，由于证书的不断更新，一段时间后同一个用户（或机构）可能会存在多个旧证书，这一系列的旧证书形成了证书的历史档案，需要对其进行归档，并集中管理，以备需要时使用。

3.4 PMI 技术

授权管理基础设施（Privilege Management Infrastructure，PMI）是国家信息安全基础设施的一个重要组成部分，目标是向用户和应用程序提供授权管理服务，提供用户身份到应用授权的映射功能，提供与实际应用处理模式相对应的、与具体应用系统开发和管理无关的授权和访问控制机制，简化具体应用系统的开发和维护。

3.4.1 PMI 的概念

PMI 是在 PKI 发展过程中为了将用户权限的管理与其公钥的管理分离，由 IETF 提出的一种标准。PKI 以公钥证书为基础，实现用户身份的统一管理；而 PMI 以 2000 年推出的 X.509 v4 标准中提出的属性证书为基础，实现用户权限的统一管理。

在过去的几年里，PKI 已成为电子商务、电子政务等网络应用中不可缺少的安全支撑系统。PKI 通过方便灵活的密钥和证书管理方式，提供了在线身份认证的有效手段，为访问控制、抗抵赖和保密性等安全机制在系统中的实施奠定了基础。随着网络应用的扩展和深入，仅仅能确定“他是谁”已经不能满足需要，安全系统要求提供一种手段能够进一步确定“他能做什么”。为了解决这个问题，PMI 应运而生。就像现实生活中一样，网络世界中的每个用户也有各种属性，属性决定了用户的权限。PMI 的最终目标就是提供一种有效的体系结构来管理用户的属性。这包括如下两个方面的含义。

（1）PMI 系统保证用户获取他们有权获取的信息，在他们的权限范围内进行相关操作。

（2）PMI 应能提供跨应用、跨系统、跨企业和跨安全域的用户属性的管理和交互手段。

概括地讲，PMI 以资源管理为核心，对资源的访问控制权统一交由授权机构统一处理。同 PKI 相比，两者的主要区别在于 PKI 证明用户是谁，而 PMI 证明这个用户有什么权限、能干什么。PMI 需要 PKI 为其提供身份认证。PMI 实际提出了一个新的信息保护基础设施，能够与 PKI 紧密地集成，并系统地建立起对认可用户的特定授权，对权限管理进行系统的定义和描述，完整地提供授权服务所需过程。

3.4.2 PMI 的组成

PMI 与 PKI 不同，PKI 主要进行身份鉴别，证明用户身份。而 PMI 主要进行授权管理，证明用户有什么权限。PMI 主要由属性权威（Attribute Authority，AA）、属性证书（Attribute Certification，AC）和属性证书库 3 部分组成。

1. 属性权威

属性权威也称为“授权管理中心”或“属性权威机构”，是整个 PMI 系统的核心，它为不同的用户和机构进行属性证书创建、存储、签发和撤销，负责管理 AC 的整个生命周期。从表面上看，PMI 中的 AA 有一些类似于 PKI 中的 CA，但两者在逻辑上是完全独立的。PKI 中的 CA 主要用来管理用户的身份，而 PMI 中的 AA 主要管理用户的权限。另外，有可能

在 PMI 建立之前 PKI 就已经存在。

图 3-10 所示的是 AA 的层次结构。其中,在该树型结构最顶端(树根)的是权威源(Source of Authority,SOA)。SOA 是授权管理的中心业务服务结点,所有的实体(包括 AA、终端用户等)都信任由 SOA 授予的部分或所有权利。在不存在授权委托的情况下,SOA 是 AC 的初始签发者,它将授权分配给授权持有者(如终端用户)。然而,如果存在着授权委托,SOA 可以授权给 AA,使得 AA 可以作为代理点,委托授权给其他实体。SOA 也可以对 AA 的权限委托施加一些限制(例如限制路径长度等)。

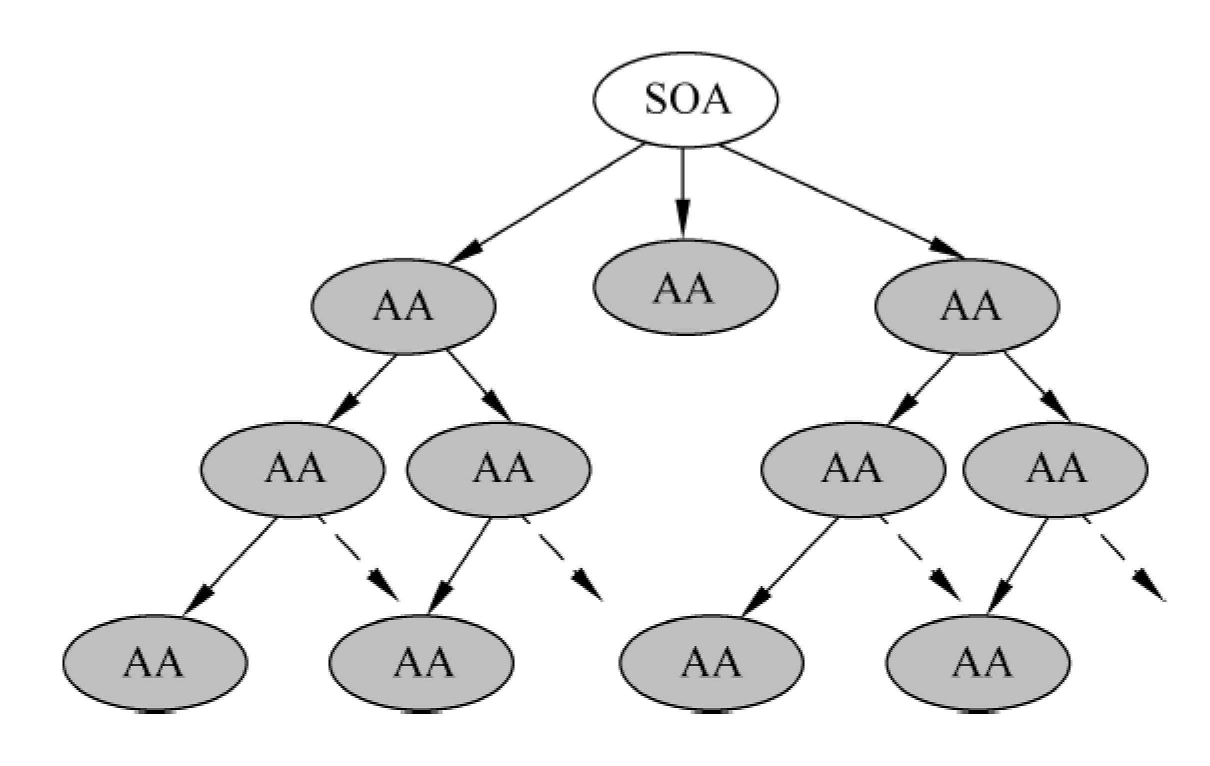


图 3-10　AA 的层次结构

在 AA 层次结构中,下一层 AA 的产生有两种情况:一种是上一层 AA 需要将某些相对独立的证书创建、颁发工作委托给一个子 AA 来担当;另外一种情况是某个已经存在的 AA 主动申请加入 PMI 系统中,并成为某一个 AA 的子节点。一般情况下,上一层 AA 充分了解自己的子节点 AA 和自己直接管理的终端用户的情况,而不一定充分了解子节点 AA 所负责管理的终端用户的情况。一般情况下,应用功能相近的终端用户可以在同一个 AA 下。

2. 属性证书

属性证书是由 PMI 的权威机构(即属性权威)签发的,将实体与其享有的权限属性捆绑在一起的数据结构。权威机构的数字签名保证了绑定的有效性和合法性。AC 主要用于授权管理。

AC 建立在基于 PKI 公钥证书的身份认证基础上。PKI 中的公钥证书保证实体及其公钥的对应性,为数据完整性、实体认证、保密性和授权等安全机制提供身份服务。那么,为什么不直接用公钥证书来加密属性而使用独立的 AC 呢?首先,身份和属性的有效时间有很大差异。身份往往相对稳定,变化较少;而属性(如职务、职位和部门等)的变化较快。因此,属性证书的生命周期往往远短于用于标识身份的公钥证书。举例来说,公钥证书类似于居民身份证,而属性证书类似于工作证。居民身份证代表了一个人的身份,签发时间一般都比较长;而工作证的有效期一般要视具体的工作单位和性质而定,时间相对比较短。

其次,公钥证书和属性证书的管理颁发部门有可能不同。仍以居民身份证和工作证为例进行说明。居民身份证实行一人一证,并由唯一的国家机关签发;而工作证可能会存在一人多证,并分别由不同的单位签发。与此相似,公钥证书由身份管理系统进行控制,而属性证书的管理则与应用紧密相关。目前,许多高校都建立了数字化校园平台,在该平台上集成了教务管理、学生管理、财务管理和资产管理等应用系统。对于学校的一个教工而言,每

人都需要一个进入数字化校园的唯一账号,该账号用于确定用户的身份。但是,不同的人员在进入数字化校园后,可能会根据工作性质的不同,对不同的系统具有不同的权限。例如,普通教师只可以访问教务系统,财务人员只可以访问财务管理系统,而学校领导则可以同时访问所有的系统。

所以,在一个系统中每个用户只有一张合法的公钥证书,而属性证书的签发则比较灵活。多个应用可使用同一属性证书,但也可为同一应用的不同操作颁发不同的属性证书。属性证书的格式如图 3-11 所示。其中的内容说明如下。

版本
主体名称
签发者
签发者唯一标识符
签名算法
序列号
有效期
属性
扩展项

图 3-11　属性证书的格式

- 版本。说明 PMI 中 AC 的版本号。具体含义与 PKI 中的数字证书相同。
- 主体名称。用于说明该授权证书的持有者。
- 签发者。签发该 AC 的 AA 名称。
- 签发者唯一标识符。签发该 AC 的 AA 的唯一标识符,以位串形式表示。
- 签名算法。签发证书时所使用的算法。
- 序列号。该证书的有效序列号,在 PMI 系统中该序列号是唯一的。
- 有效期。该证书的有效使用期限。
- 属性。拥有者所具有的权限属性。
- 扩展项。用于功能的扩展。

PMI 中属性证书的撤销与 PKI 中公钥证书相似,也是通过证书撤销列表的方式来实现的。在 PMI 系统中,需要维护 ACRL(属性证书撤销列表)来进行证书的撤销操作。

3. 属性证书库

属性证书库用于存储属性证书,一般情况下采用 LDAP 目录服务器,主要出于以下几点考虑。

(1) 由于 LDAP 目录服务器能够处理大量的用户并发,这样便于属性证书的检索,并具有更快的响应速度。

(2) LDAP 目录服务器具有完善的安全机制,可以通过访问控制列表设置对目录数据读和写的权限。通过支持基于 SSL 的安全机制完成对明文的加密,可以为属性证书的管理提供安全保障。

(3) LDAP 目录服务器可以跨平台操作,支持 Windows、UNIX、Linux 和 NetWare 等几乎所有的主流操作系统。

(4) 同步复制功能。例如,分布在不同地理位置的两台目录服务器可以通过使用“推”、“拉”技术使服务器保持数据的同步和一致。

(5) LDAP 目录服务器数据的组织方式采用树形层次结构,便于扩展。

3.4.3　基于角色的访问控制

随着现代信息技术的迅速发展,在网络中传输和处理的信息和数据越来越多。对于一个资源可控的网络来说,在资源数量迅速扩大的同时需要加强对资源的控制和管理。

在分布式网络环境下,对于安全性要求较高的信息资源,既要求能够由信息资源的管理

部门统一进行管理，确保信息资源受控、合法和安全地使用，又需要授权管理和访问控制的复杂度不能因为资源和用户数量的增长而迅速增加，以确保授权和访问控制的可管理性，实现统一、高效和灵活的访问控制。传统的访问控制机制主要有自主访问控制(Discretionary Access Control，DAC)和强制访问控制(Mandatory Access Control，MAC)。

其中，自主访问控制也叫做基于身份的访问控制，其主要思想是系统的主体可以自主地将其拥有的对客体的访问权限授予其他主体，且这种授予具有可传递性。特点是灵活性高，但授权管理复杂，安全性低。而强制访问控制也叫基于规则的访问控制，其主要思想是将主体和客体分级，根据主体和客体的级别标识来决定访问控制。特点是便于管理，但灵活性差，完整性方面控制不够。

随着网络应用的不断发展，传统的 DAC 和 MAC 两种访问控制方式已远远不能满足访问控制的上述要求。20 世纪 90 年代以来发展起来的基于角色的访问控制(Role-Based Access Control，RBAC)技术可以减少授权管理的复杂度，降低管理开销，提高访问控制的安全性，而且能够实现基于策略的授权管理和访问控制。

以资源分配管理为主的 PMI 系统，其授权管理是基于角色的。角色是给用户分配权限的一种间接手段，是对用户拥有的职能和权限的一种抽象。通过定义角色，为每个角色分配一定的权限。RBAC 的基本思想是：根据用户在组织内的职称、职务及所属的业务部门等信息来定义用户拥有的角色。而授权给用户的访问权限，由用户在组织中担当的角色来确定。

鉴于基于角色的访问控制技术的优势，需要在 PMI 中采用基于角色的访问控制技术进行授权管理和访问控制。具体以角色为中介，建立以对象与操作、权限、角色、组织结构、系统结构为核心的层次化的资源结构和关系的描述、定义和管理框架，充分反映信息系统资源配置和部署的现状，以及未来资源结构动态变化和业务发展的需求，为授权管理和访问控制提供基础信息，并通过角色的分配实现对用户的授权，提高授权的可管理性和安全性，简化授权管理的复杂度，降低资源管理和授权管理的成本，提高管理的效率。

与传统的访问控制机制相比，在 PMI 系统中基于角色的授权管理模式主要存在以下三个方面的优势。

(1) 授权管理的灵活性。基于角色的授权管理模式可以通过属性证书的有效期，以及委托授权机构来灵活地进行授权管理，从而实现传统的访问控制技术领域中的强制访问控制模式与自主访问控制模式的有机结合，其灵活性要优于传统的授权管理模式。

(2) 授权操作与业务操作相分离。基于角色的授权管理模式将业务管理工作与授权管理工作完全分离，更加明确了业务管理员和安全管理员之间的职责分工，可以有效地避免由于业务管理人员参与到授权管理活动中可能带来的一些问题。

(3) 多授权模型的灵活支持。基于角色的授权管理模式将整个授权管理体系从应用系统中分离出来，授权管理模块自身的维护和更新操作将与具体的应用系统无关。因此，可以在不影响原有应用系统正常运行的前提下，实现对多授权模型的支持。

3.4.4 PMI 系统框架

授权管理基础设施在体系上可以分为三级：权威源(SOA)、属性权威和 AA 代理点。在实际应用中，这种分级体系可以根据需要进行灵活配置，可以是三级、二级或一级。PMI 系统的基本框架如图 3-12 所示。

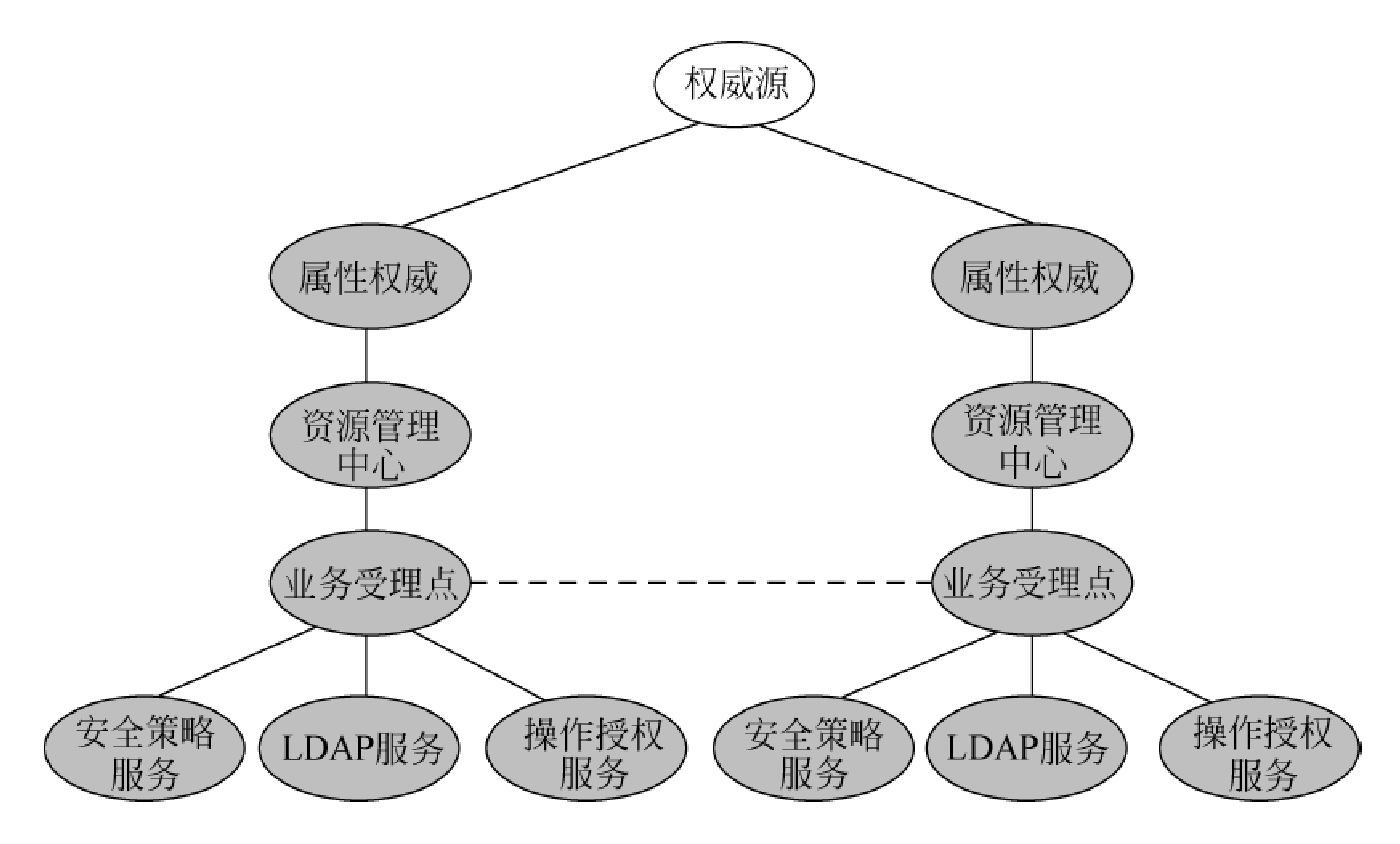


图 3-12　PMI 系统框架

1. 权威源

权威源是整个授权管理体系的中心业务节点，也是整个授权管理基础设施的最终信任源和最高管理机构。SOA 的职责主要包括授权管理策略的管理、应用授权受理、AA 的设立审核和管理，以及授权管理体系业务的规范化等。

2. 属性权威

属性权威是授权管理基础设施的核心服务节点，是对应于具体应用系统的授权管理分系统，由具有设立 AA 业务需求的各应用单位负责建设，并与 SOA 中心通过业务协议达成相互的信任关系。AA 的职责主要包括应用授权受理、属性证书的发放和管理，以及 AA 代理点的设立审核和管理等。AA 需要为其所发放的所有 AC 维持一个历史记录和更新记录。

3. AA 代理点

AA 代理点是授权管理基础设施的用户代理节点，也称为"资源管理中心"。AA 代理点与具体应用直接联系，是对应 AA 的附属机构，接受 AA 的直接管理，由各 AA 负责建设，但必须经过 SOA 的同意，并签发相应的证书。AA 代理点的设立和数目由各 AA 根据自身的业务发展需求而定。AA 代理点的职责主要包括应用授权服务代理和应用授权审核代理等，负责对具体的用户应用资源进行授权审核，并将 AC 的操作请求提交到 AA 进行处理。

4. 访问控制执行者

访问控制执行者是指用户应用系统中具体对授权验证服务的调用模块。实际上访问控制执行者并不属于授权管理基础设施的部分，但却是授权管理体系的重要组成部分。

访问控制执行者的主要职责是将最终用户针对特定的操作授权所提交的授权信息，连同对应的身份验证信息（公钥证书）一起提交到 AA 代理点，并根据 AA 返回的授权结果，进行具体的应用授权处理。

3.4.5　PMI 与 PKI 之间的关系

在建设 PMI 设施时，必须拥有足够安全性的 PKI 设施。其中，PKI 负责公钥信息的管理，而 PMI 负责权限的管理。PMI 设施中的每一个 AA 实体和终端用户都是 PKI 设施的用户，所以从应用角度来看，PMI 和 PKI 的发展是相辅相成并互为条件的。虽然 PMI 是在

PKI 的基础上提出的，但是 PMI 的应用和发展离不开 PKI 设施的支持。

可以将 PMI 和 PKI 绑定在一起，也可以让 PMI 与 PKI 在物理上分开。因为与 PMI 相比，PKI 相对比较稳定，其属性的变化较小。而 PMI 则会因为应用类型的变化（如增加或删除）而动态更新。所以 PMI 在逻辑上必然与 PKI 相联系，而在物理上可分离也可合并。

PMI 和 PKI 有很多相似的概念。如属性证书与公钥证书，属性权威与认证机构。公钥证书是对用户名称和其公钥进行绑定，而属性证书是将用户名称与一个或更多的权限属性进行绑定。数字签名公钥证书的实体称为 CA，签名属性证书的实体称为 AA。PKI 和 PMI 之间的主要区别在于：PMI 主要进行授权管理，证明这个用户有什么权限，能干什么，即“你能做什么”；而 PKI 主要进行身份鉴别，证明用户身份，即“你是谁”。将 PKI 和 PMI 技术结合，实现可信的身份认证和可信授权管理是目前较为完善的安全保障措施。

3.5 实验操作 1 数字证书的应用

本章前面的内容较为详细地介绍了 PKI 和 PMI 的相关知识，本节通过一个具体的实验，使读者在掌握数字证书的应用方法和特点的同时，对本书第 2 章介绍的数据加密技术和本章的 PKI 和 PMI 技术有一个较为直观的认识。

为了便于实验，本节直接使用了 Internet 上的认证系统进行介绍。当然，读者可以自己安装一台证书服务器来为用户提供证书服务。例如，可利用 Windows Server 2003 操作系统提供的“证书服务”功能来安装一台单位内部使用的证书服务器，其应用方法和效果与下面的介绍基本相同。

3.5.1 数字证书的获取

数字证书可以通过证书认证机构获得。有些证书认证机构是面向所有网络用户的，例如网证通 NETCA 电子认证系统（https://testca.netca.net），如图 3-13 所示，而有些是由公司内部自行创建的，如银行的数字证书，这些证书必须经申请后才能够获取。

获得免费数字证书的方法很多，目前国内有很多 CA 中心提供试用型数字证书，其申请过程在网上即时完成，并可以免费使用。

（1）在浏览器中输入 https://testca.netca.net，打开如图 3-13 所示的主页面后，单击“证书申请”链接，在打开的如图 3-14 所示的页面中单击“试用型个人数字证书申请”链接。



图 3-13 一个可提供免费数字证书的机构



图 3-14 证书申请

（2）由于只有安装了根证书（证书链）的计算机，才能完成后面的申请步骤和正常使用用户在 CA 中心申请的数字证书，所以在出现如图 3-15 所示的页面时，单击“安装证书链”按钮。

网证通 NET CA 申请试用型个人数字证书

特别提示

只有安装了试用CA证书链的计算机，才能完成后面的申请步骤和正常使用您在本中心申请的数字证书。

请您点击以下"安装证书链"图标，如果您没有安装过本公司的试用型根证书，那么系统将提示您是否将证书添加到根证书存储区，请选择"是"。然后系统将自动将CA证书链安装到您的计算机上，安装完成后系统将提示您证书下载完毕。点击"确定"即可。

在成功安装试用CA证书链后，请您点击"继续"图标，进行下一步操作。

安装证书链　继　续

返回页首

图 3-15　安装证书链

(3) 按照表单上的提示，输入完整的个人资料。选择加密服务提供程序(Cryptographic Service Provider，CSP)，其中 CSP 负责创建密钥、吊销密钥，以及使用密钥执行各种加、解密操作。每个 CSP 都提供了不同的实现方式。某些提供了更强大的加密算法，而另一些则包含硬件组件，例如智能 IC 卡或 USB 电子令牌。当用户使用特别的数字证书存储介质(如智能 IC 卡或 USB 电子令牌)存储数字证书及其相应的私有密钥时，可以在"CSP(加密服务提供程序)"下拉列表中选择该存储介质生产厂商提供的 CSP，如图 3-16 所示。本例可以选择 Microsoft Base Cryptagraphic Provider v1.0 选项。



图 3-16　选择 CSP

补充信息可以选填有效证件类型、证件号码、用户的出生日期、用户的性别、用户的住址、通信地址、通信所在地邮政编码、联系电话、传真号码和存储介质等。然后单击"继续"按钮提交。申请成功后，出现如图 3-17 所示的界面，请用户牢记该证书的业务受理号和密码。



图 3-17　申请成功后的提示信息

(4) 单击图 3-17 中的"安装证书"按钮后，系统弹出一个认证界面，要求用户再次输入证书的业务受理号和密码，用户只需要将图 3-17 中申请到的号码输入即可。之后，出现如

图 3-18 所示的提示信息。



图 3-18　用户的数字证书

（5）单击“安装证书”按钮，开始从 CA 中心下载证书到用户的计算机上，并进行安装。结束后出现如图 3-19 所示的提示信息。

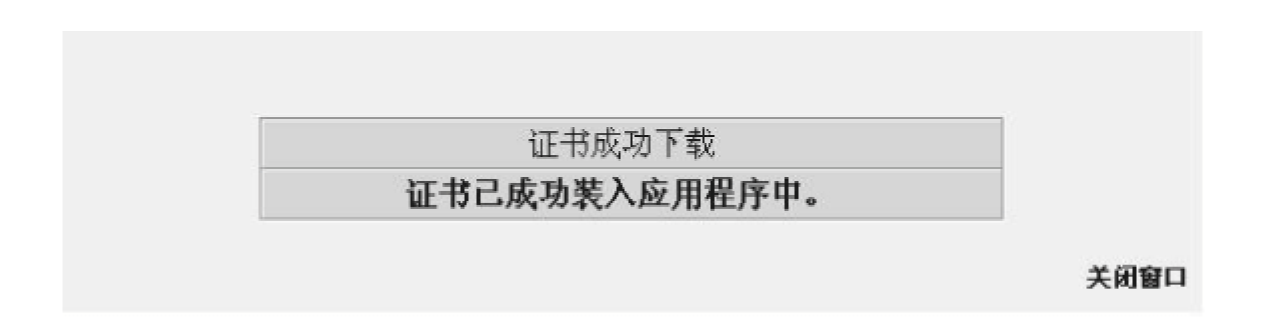


图 3-19　证书已成功安装

（6）在 IE 中查看数字证书。通过 IE 浏览器自带的数字证书管理器，可以看到已安装的数字证书。具体方法是在打开 Internet Explorer 后，选择“工具”→“Internet 选项”命令，在打开的“Internet 选项”对话框中选择“内容”选项卡，打开如图 3-20 所示的对话框。单击“证书”按钮，在打开的如图 3-21 所示的“证书”对话框中就可以看到当前证书的列表。



图 3-20　“Internet 选项”对话框中的“内容”选项卡

选定要查看的个人数字证书，然后单击“查看”按钮，在打开的如图 3-22 所示的“证书”对话框中可以查看证书的详细信息。




图 3-21　显示当前的证书列表

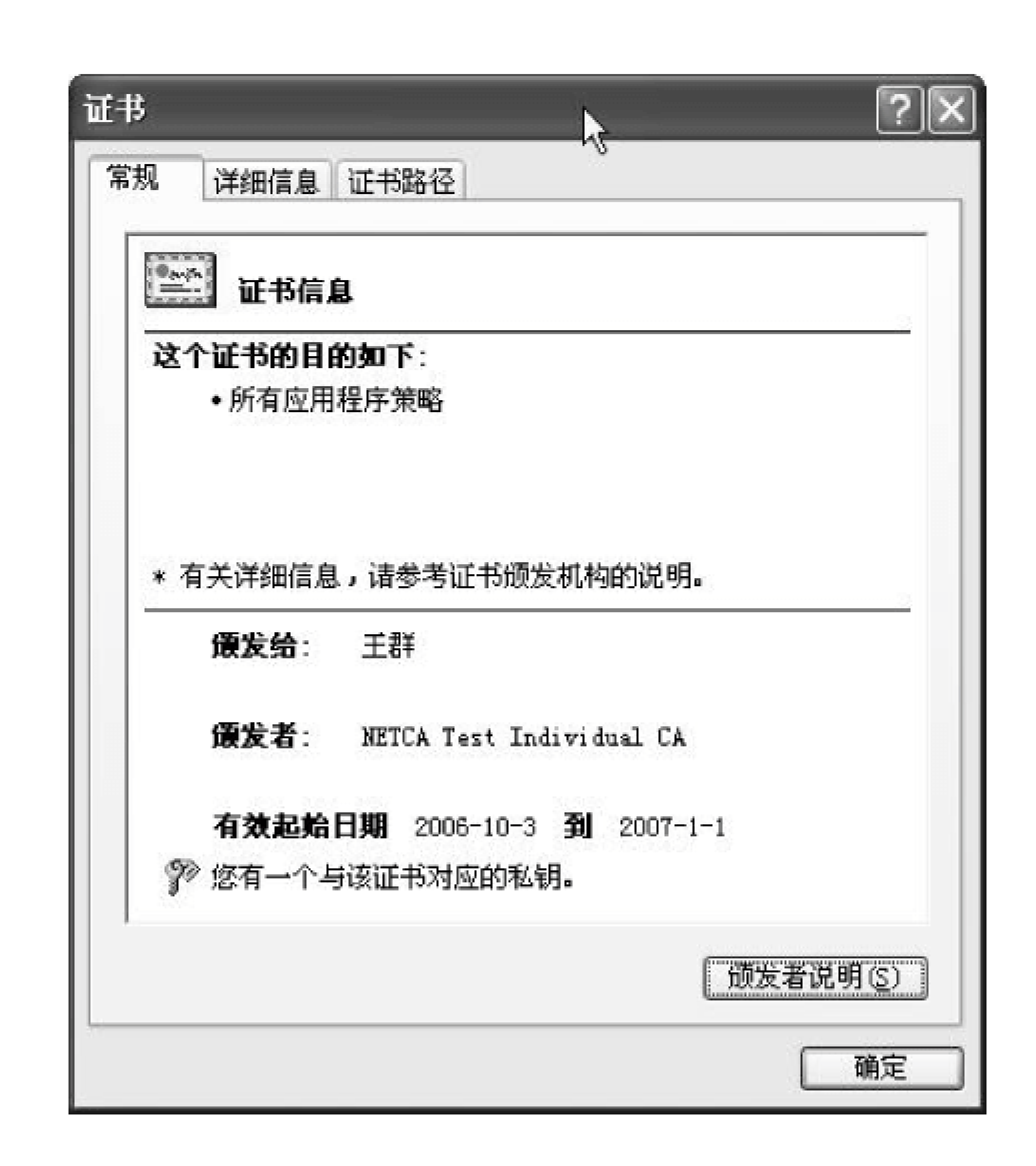


图 3-22　查看数字证书的详细信息

有了数字证书以后,可以发送安全的电子邮件,实现网上邮件的加密和签名电子邮件,还可以应用于公众网络上的商务活动中,应用范围涉及需要身份认证及数据安全的各个行业和领域,如访问安全站点、网上签约、网上订购和网上办公等网上的安全电子事务处理和安全电子交易活动。随着信息化进程的不断加快,数字证书的颁发机构中心将作为一种基础设施为信息的交换提供可靠的保障。

3.5.2　用电子邮件验证数字证书的应用

下面以数字证书在电子邮件中的应用为例,介绍数字证书的使用方法和特点。安全电子邮件证书中包含证书持有者的电子邮件地址、公钥及 CA 中心的签名。使用安全电子邮件证书可以收发经过加密和数字签名的邮件,保证电子邮件传输中的机密性、完整性和不可否认性,确保电子邮件通信各方身份的真实性。证书可以存储在硬盘或 U 盘中。安全电子邮件利用公钥算法保证用户的签名邮件不会被篡改,而用户的加密邮件除了邮件接收者以外的任何人都无法阅读其中的内容。

需要注意的是,证书中的邮件地址必须与绑定的邮件账号一致,这样就可以对自己的邮件进行签名和加密。

下面以 Outlook Express 为例,利用前面已申请到的数字证书来实现安全电子邮件的收发。在具体设置之前,首先在如图 3-21 所示的"证书"对话框中选取已安装的数字证书名称,单击"高级"按钮,在打开的如图 3-23 所示的"高级选项"对话框的"证书目的"列表中勾选"安全电子邮件"复选框。



图 3-23　选取"安全电子邮件"复选框

1. 设置邮箱地址

(1) 打开 Outlook Express,然后选择"工具"→

“账户”命令，打开“Internet 账户”对话框，选择“添加”→“邮件”选项，如图 3-24 所示。



图 3-24 添加邮件账户

（2）在打开的如图 3-25 所示的“Internet 连接向导”对话框的“显示名”文本框中输入用户的邮件显示姓名。



图 3-25 输入电子邮件显示名称

（3）单击“下一步”按钮，在打开的如图 3-26 所示的对话框的“电子邮件地址”文本框中输入用户的电子邮件地址名称，如 wq@etongtv.net。

（4）单击“下一步”按钮，在打开的如图 3-27 所示的对话框中分别输入接收邮件服务器和发送邮件服务器的域名或 IP 地址，本例为 mail.etongtv.net。不同电子邮件系统的设置可能不同，请用户参阅相关的说明文档。

（5）单击“下一步”按钮，在出现的如图 3-28 所示的对话框中输入该邮箱的密码。

（6）单击“下一步”按钮，完成设置。新添加的邮箱地址如图 3-29 所示。

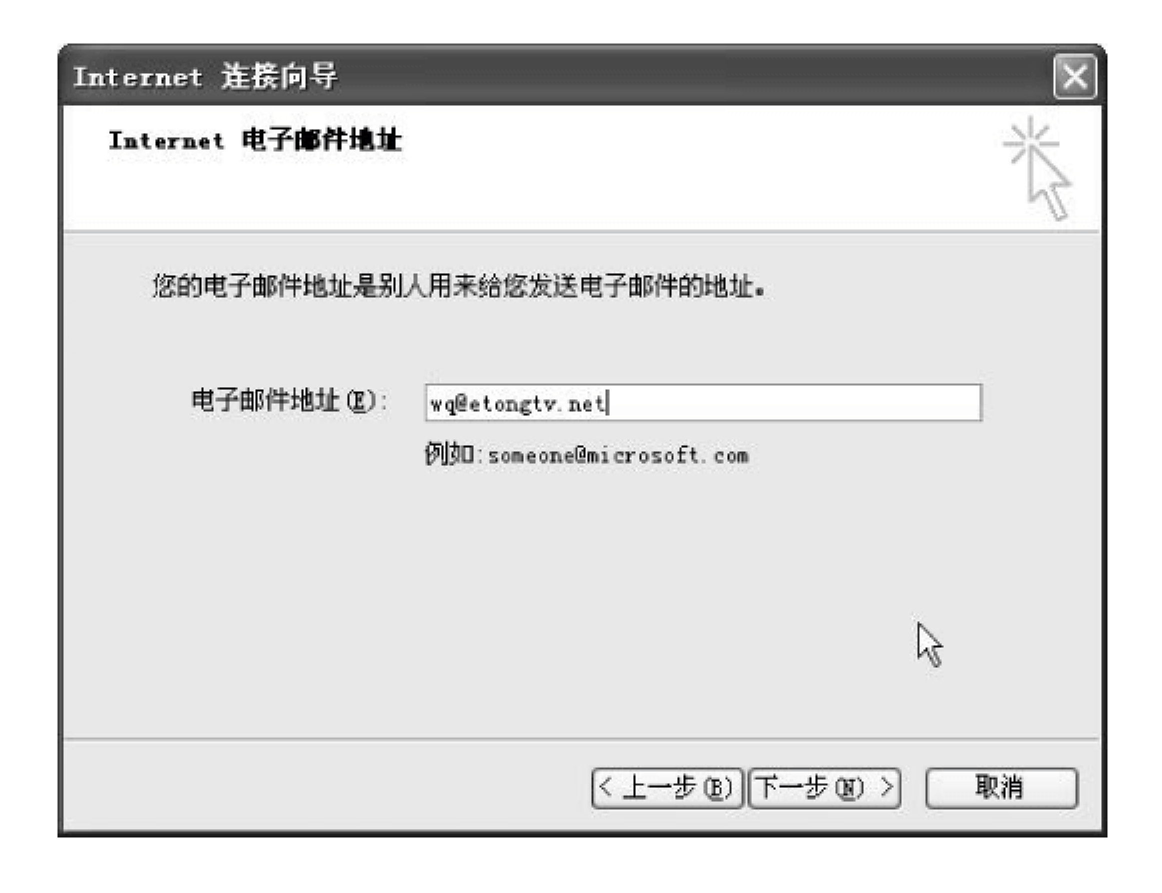


图 3-26　输入电子邮件地址



图 3-27　设置电子邮件服务器域名或 IP



图 3-28　输入邮箱的用户密码



图 3-29　显示已添加的邮箱账户名称

2. 设置邮箱与数字证书的绑定

(1) 打开 Outlook Express，选择“工具”→“账号”命令，在打开的如图 3-29 所示的“Internet 账户”对话框中，选取已创建的用于发送安全电子邮件的邮箱账号。然后单击“属性”按钮，打开如图 3-30 所示的对话框，可以看到“签署证书”和“加密首选项”选项区域，通过相关设置，可以进行邮件的签名和加密。

(2) 单击“签署证书”选项区域中的“选择”按钮，在打开的如图 3-31 所示的“选择默认账户数字 ID”对话框中可以看到在 https://testca.netca.net 上已申请到的数字证书。选取数字证书名称，单击“确定”按钮，完成邮箱与证书的绑定。

注意，如果在如图 3-31 所示的对话框中没有显示相关的证书，请确认用户的证书已经正确安装且没有过期。同时要确认用户在 Outlook Express 中所设置的邮箱与用户在申请数字证书时所提供的邮箱一致。查看在申请数字证书时所提供邮箱的方法为：在 Internet Explorer 中，依次选择“工具”→“Internet 选项”命令，在打开的对话框中选择“内容”选项卡，单击“证书”按钮，在打开的对话框中选取用户的数字证书，选择“查看”→“详细信息”命令，在打开的如图 3-32 所示的“证书”对话框中就可以看到邮箱名称。

(3) 按照同样的方法，可以在“加密首选项”选项区域中添加用户自己的证书，最后如图 3-33 所示。



图 3-30　设置邮箱的安全属性



图 3-31　选择要使用的数字证书



图 3-32　查看申请证书时使用的邮箱名称

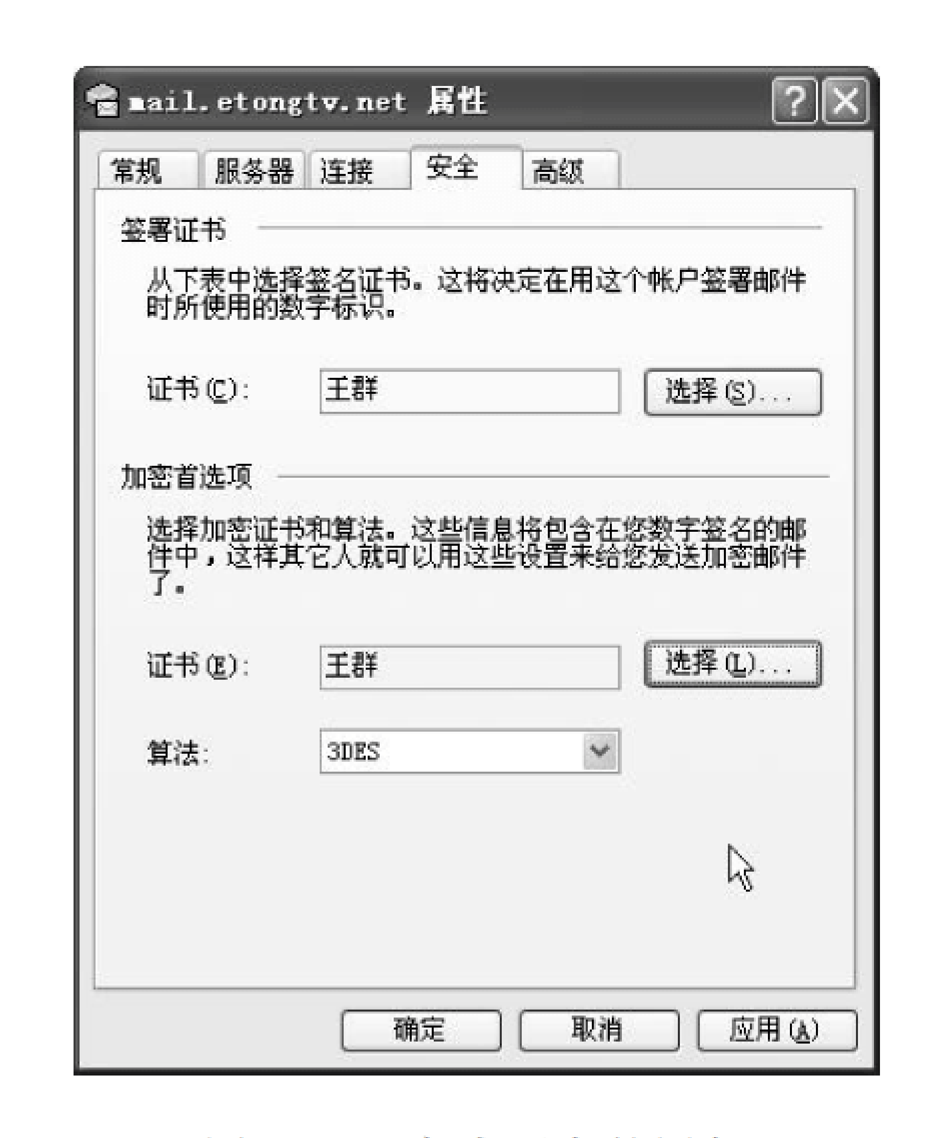


图 3-33　完成证书的添加

(4) 单击“确定”按钮，完成邮箱与数字证书之间的绑定操作。

3. 对电子邮件进行签名

发送加密邮件前必须先获得接收方的数字标识，用户可以首先让接收方给自己发一份签名邮件来获取对方的数字标识，或者直接到 CA 中心的网站(本例为 http://www.cnca.net)去查询下载来获取对方的数字标识。

注意，也许有读者会问：使用邮件来向对方发送数字证书难道不存在安全隐患吗？答案是肯定的。解决这一问题，就需要考虑证书的管理问题，即如何安全地发送和保存数字证书。此方面的内容请读者阅读相关的资料。

(1) 打开 Outlook Express，选择“新邮件”，撰写一份新的电子邮件。在发送之前单击窗口右上方的“签名”或“加密”选项(本例同时进行了“签名”和“加密”)，如图 3-34 所示。

(2) 单击“发送”按钮，签名邮件发送成功。当收件人收到并打开有数字签名的邮件时，



图 3-34　对邮件进行签名和加密处理

将看到“数字签名邮件”的提示信息，单击“继续”按钮后，才可阅读到该邮件的内容，如图 3-35 所示。

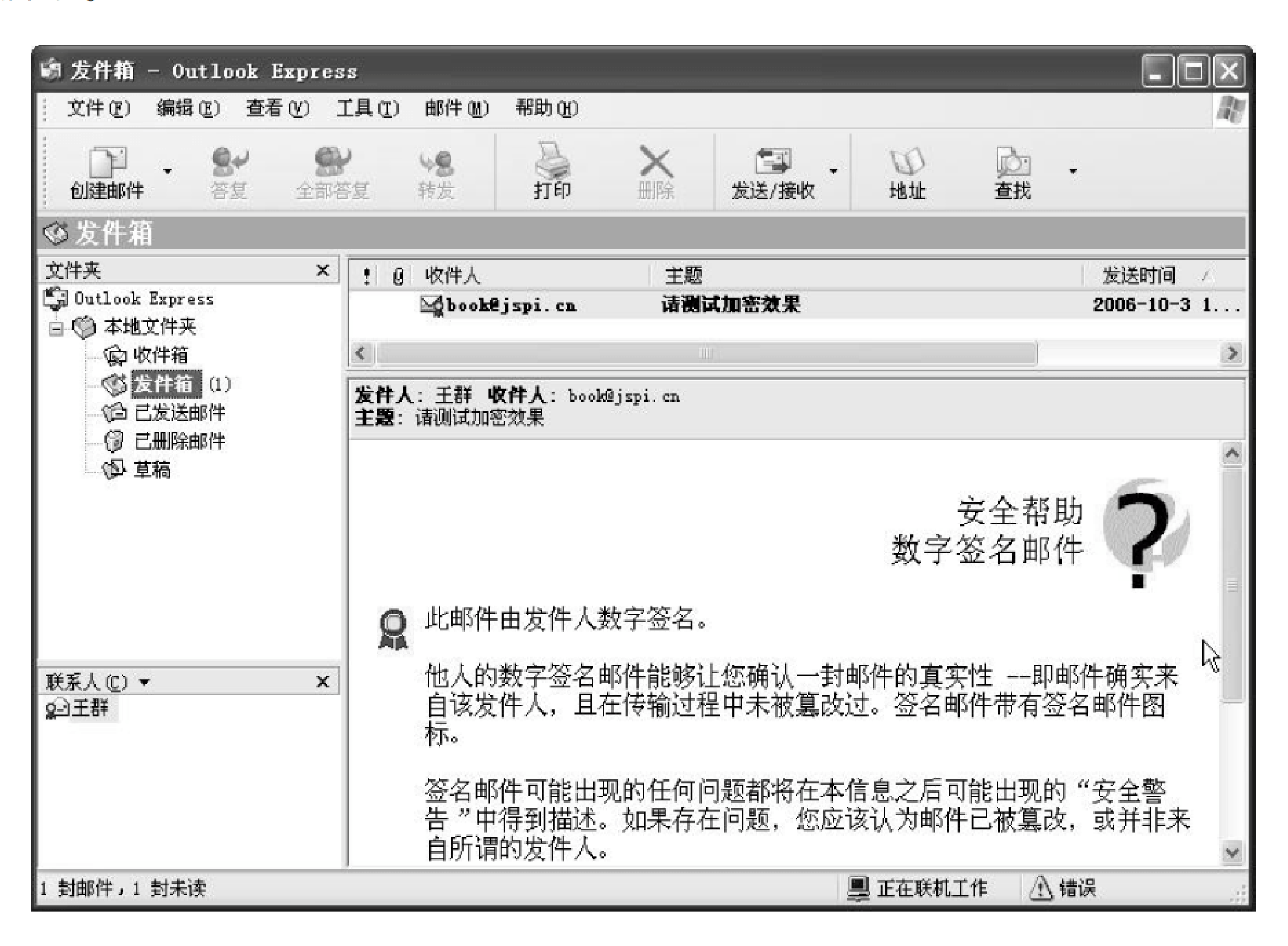


图 3-35　已签名的电子邮件

如果邮件在传输过程中被他人篡改或发信人的数字证书有问题，将出现“安全警告”提示。收到邮件后可以看到，邮件的右边中间有一个小图标，单击该图标就可以看到相关的数字证书信息，如图 3-36 所示。另外，可以单击“查看证书”按钮来查看该签名邮件的证书信息。

如果在发送加密邮件时没有得到接收方的数字标识，将会出现如图 3-37 所示的提示信息，发送方只能在单击了“不要加密”按钮后才能发送。接收方收取加密的电子邮件实际上是一个解密的过程，相关算法已经隐藏在后台运行。



图 3-36　查看邮件的证书



图 3-37　未得到接收方数字标识时的提示信息

通过前面安全电子邮件的介绍，相信读者对加密、签名等安全技术的应用有了一个初步的认识，并增强了对本章前面理论知识的理解。

习　　题

3-1　什么是 PKI？PKI 与数据加密算法之间存在什么关系？PKI 主要解决网络安全中的什么问题？

3-2　从消息的保密性、完整性、真实性和不可否认性等方面，分析 PKI 与网络安全之间的关系。

3-3　从 PKI 策略、认证机构 CA、注册机构 RA、证书发布系统和 PKI 应用等方面，分析 PKI 系统的特点。

3-4　在 PKI 系统中，CA 的作用是什么？

3-5　结合实际应用，从安全服务器、注册机构 RA、CA 服务器、LDAP 目录服务器和数

据库服务器等方面，分析 CA 各组成部分的功能特点。

3-6 联系实际，说明 CA 之间是如何建立信任关系的，并分析不同 CA 之间信任模型的特点。

3-7 什么是数字证书？在网络安全中数字证书的作用是什么？

3-8 详细分析数字证书的签发和撤销方式。

3-9 在 PKI 系统中为什么要进行数字证书的更新操作？如何实现？

3-10 联系 PKI 技术，介绍 PMI 的概念和应用特点。

3-11 什么是基于角色的访问控制方式？

3-12 联系实际应用，分析 PKI 与 PMI 之间的关系。

3-13 通过实验，掌握数字证书的使用方法。

第 4 章　身份认证技术

身份认证也称为“身份验证”或“身份鉴别”，是指在计算机及计算机网络系统中确认操作者身份的过程。相信读者都听说过这个经典的故事：一条狗在计算机前一边打字一边对另一条狗说：“在因特网上，没有人知道你是一个人还是一条狗！”这个故事听起来虽然颇具讽刺意味，但却说明了一个问题：在因特网上身份识别的重要性和迫切性。计算机系统和计算机网络系统是一个虚拟的数字世界。在这个虚拟数字世界中，包括用户身份的一切信息都是用 0 和 1 组成的特定数据来表示，计算机只能识别用户的数字身份。所以，对用户的授权也是针对用户数字身份进行的。本章将较为系统地介绍身份认证的相关技术及实现方法。

4.1　身份认证概述

对于一个要求确认彼此身份的完整通信过程来说，身份认证是通信前首先要完成的一项工作。身份认证机制可以识别网络中各实体的身份，防止出现身份欺诈，保证参与通信的实体之间身份的真实性。

4.1.1　身份认证的概念

身份认证（Authentication）是系统审查用户身份的过程，从而确定该用户是否具有对某种资源的访问和使用权限。身份认证通过标识和鉴别用户的身份，提供一种判别和确认用户身份的机制。身份认证需要依赖其他相关技术，确认系统访问者的身份和权限，使计算机和网络系统的访问策略能够可靠、有效地执行，防止攻击者假冒合法用户获得资源的访问权限，从而保证系统和数据的安全，以及授权访问者的合法利益。

计算机网络中的身份认证是通过将一个证据与实体身份绑定来实现的。实体可能是用户、主机、应用程序甚至是进程。证据与身份之间是一一对应的关系，双方通信过程中，一方实体向另一方实体提供这个证据证明自己的身份，另一方通过相应的机制来验证证据，以确定该实体是否与证据所显示的身份一致。

身份认证技术在信息安全中处于非常重要的地位，是其他安全机制的基础。只有实现了有效的身份认证，才能保证访问控制、安全审计和入侵防范等安全机制的有效实施。随着电子商务、网上支付和网上银行等业务的快速发展，账户被盗用的事件频繁发生，用户对于使用网络进行商务和支付缺少安全感，使得计算机网络在这些领域的发展受到限制。提供安全的身份认证方法是解决这些问题的关键。

在现实生活中每一个人都有一个真实的物理身份，如居民身份证、户口本等。在计算机

网络中如何保证以数字代码来标识用户身份时的真实性呢？如何通过技术手段保证用户的物理身份与数字身份是一致的呢？这便是身份认证要解决的问题。在真实世界中，验证一个用户的身份主要通过以下三种方式。

(1) 所知道的。根据用户所知道的信息(what you know)来证明用户的身份。假设某些信息只有某个用户知道，如暗号、知识和密码等，通过询问这个信息就可以确认这一用户的身份。

(2) 所拥有的。根据用户所拥有的东西(what you have)来证明用户的身份。假设某一样东西只有某个用户拥有，如印章、身份证、护照和信用卡等，通过出示这些东西也可以确认用户的身份。

(3) 本身的特征。直接根据用户独一无二的体态特征(who you are)来证明用户的身份，例如人的指纹、笔迹、DNA、视网膜及身体的特殊标志等。

在以上三种验证身份的方式中，只有本身的特征是独一无二且不可伪造的，而其他两种方式都会存在安全风险。在网络环境中，身份认证一般有多种方式。例如，当用户通过银行的 ATM(自动柜员机)取款时，首先要插入银行卡(所拥有的)，然后再输入其密码(所知道的)，当两个条件同时具备时才能够在 ATM 上取到钱。但是，这两个条件都具有安全风险，银行卡可能会丢失，捡到银行卡的人可能会猜到或通过其他手段得到其密码。但是，如果这里的组合不是“银行卡＋密钥”，而是“银行卡＋指纹”或“银行卡＋视网膜”，那么系统的安全性将会高出许多。当然，在网络世界里没有绝对的安全，无论采取哪一种或哪一些安全认证方式，总会存在相应的安全风险。

4.1.2 认证、授权与审计

在本书的第 3 章介绍了“访问控制”的概念，用它来表示与系统资源访问相关的问题。在这个定义中涉及到了认证和授权两部分内容。在计算机网络安全领域，将认证、授权与审计统称为 AAA 或 3A，即 Authentication(认证)、Authorization(授权)和 Accounting(审计)。

1. 认证

认证是一个解决确定某一个用户或其他实体是否被允许访问特定的系统或资源的问题。在网络中，任何一个用户或实体在进行任何操作之前，必须要有相应的方法来识别用户或实体的真实身份。为此，认证又称为鉴别或确认。身份认证主要鉴别或确认访问者的身份是否属实，以防止攻击，保障网络安全。

2. 授权

授权是指当用户或实体的身份被确定为合法后，赋予该用户的系统访问或资源使用权限。只有通过认证的用户才允许访问系统资源，然而在许多情况下，当一个用户通过认证后通常不可能赋予访问所有系统资源的权限。例如，在 Windows 操作系统中，通过认证的系统管理员账户(Administrator)可以对系统配置进行设置，而通过认证的临时账户(Guest)只能查看系统的一些基本信息。为此，必须根据用户身份的不同，给不同的用户授予不同的权限，限制通过认证的用户的行为。

3. 审计

审计也称为记账(accounting)或审核，出于安全考虑，所有用户的行为都要留下记录，以便进行核查。所采集的数据应该包括登录和注销的用户名、主机名及时间。对于安全要

求较高的网络，审计数据应该包括任何人所有的试图通过身份认证和获得授权的尝试。另外，对于以匿名(anonymous)或临时账户身份对公共资源的访问情况也应该进行采集，以便于进行安全性评估时使用。

安全性评估(security assessment)是审计操作的进一步扩展。在安全性评估中，专业人员对网络中容易受到入侵者攻击的部分进行内部检查，对网络存在的薄弱环节进行阶段性评估。通过对评估结果的分析，既可以发现网络中存在的设计缺陷，也可以为今后的网络调整提供权威的数据支撑。

用户对资源的访问过程如图 4-1 所示。

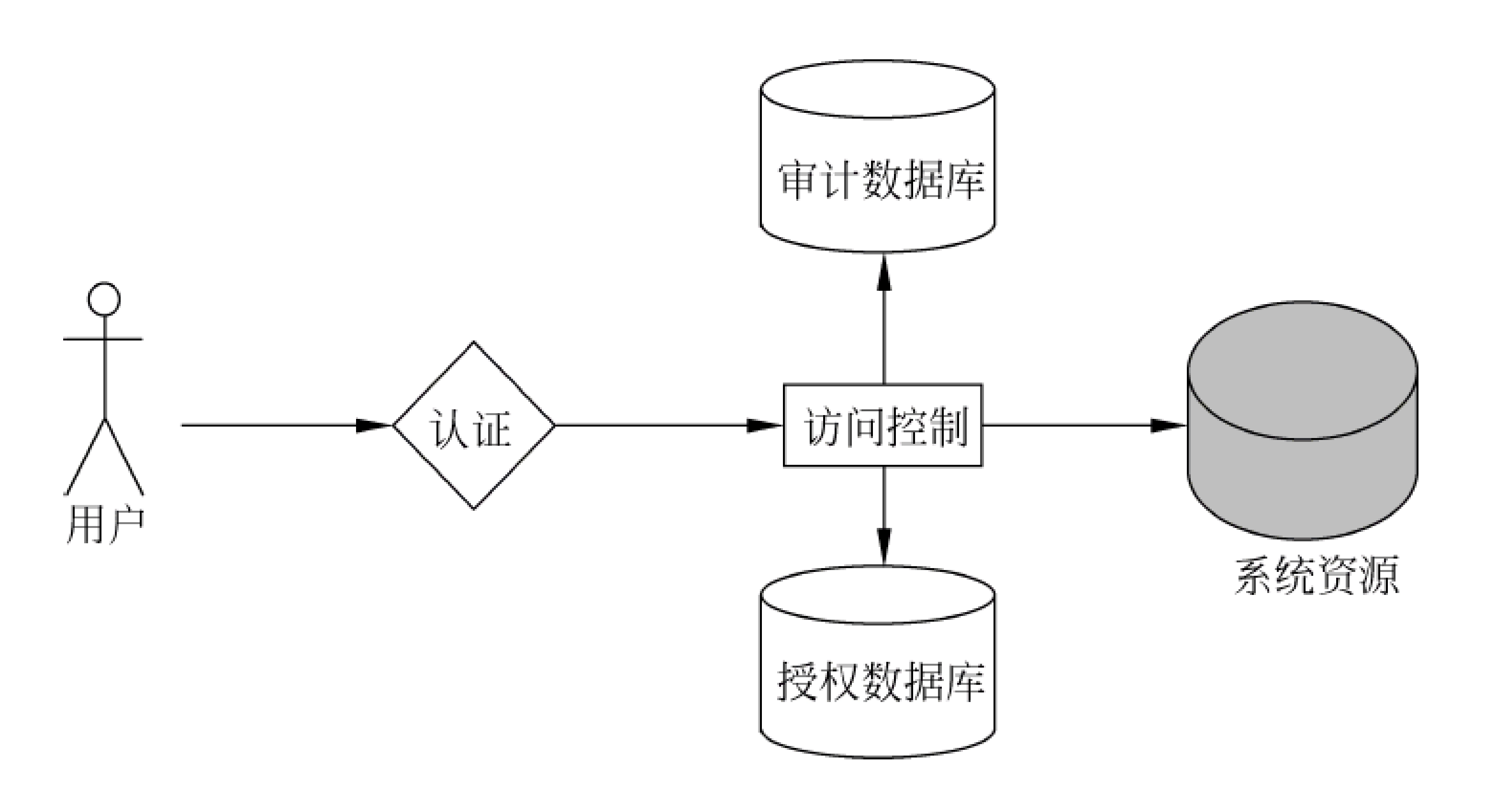


图 4-1　用户访问系统资源的过程

4.2　基于密码的身份认证

密码认证也称为“口令认证”，它是计算机系统和网络系统中应用最早也最为广泛的一种身份认证方式。

4.2.1　密码认证的特点

密码是用户与计算机之间及计算机与计算机之间共享的一个秘密。在通信过程中，其中一方向另一方提交密码，表示自己知道该秘密，从而通过另一方的认证。密码通常由一组字符串来组成，为便于用户记忆，一般用户使用的密码都有长度的限制。但出于安全考虑，在使用密码时需要注意以下几点。

(1) 不使用默认密码。许多系统和软件都提供了一些初始用户账号和密码，例如许多系统的初始用户账户为 Administrator 或 Admin，对应的密码为 password 或干脆为空(即没有密码)。为了提高系统的安全性，建议用户不要使用这些默认账户及密码，更不能使用空密码。

(2) 设置足够长的密码。密码至少应该包含有 6 个以上的数字或字母，一般来说密码越长越安全，这主要是为了减少密码被暴力破解的几率。

(3) 不要使用结构简单的词或数字组合。不管是什么语言的名称或是单词，都可以通过一些专门的扫描程序快速猜出密码。

(4) 增加密码的组合复杂度。密码中尽量包含有数字、标点、下划线及大小写字母。从安全角度考虑，凡是能使用户的密码变得难以破解的一切手段都是可取的。

(5) 使用加密。一般情况下不建议用户将密码写在纸上或以文件的形式存放在计算机中。如果用户必须写下密码的话，应该将其放在加密的文件夹里。另外，还有一些专门的密码管理软件可以帮助网络管理员管理大量的设备或系统密码。

(6) 避免共享密码。不同的设备或系统使用不同的密码。当同一个设备或系统被多个用户管理时，建议创建各自的密码，而不要共享。

(7) 定期更换密码。定期更换密码是十分有必要的。一般建议用户至少应该三个月更换一次密码，对于保密要求很高的设备和系统而言，可以使用一次性密码。

因为密码认证易于管理、操作简单，而且不需要额外的成本，用户只要记得账号与密码，就可以进行系统资源的访问。所以，为了防止非法用户进入计算机系统，最常用的方法是密码认证，以保护计算机或网络系统不被入侵者破坏。合法用户利用正确的密码，可以登录计算机和网络系统，非法的用户则被拒之门外。

传统的密码认证方式是先建立用户账户，然后为每一个用户账户分配一个密码。用户登录首先发送一个包含用户账户与密码的请求登录信息，主机系统根据储存在用户数据库中的用户账户与密码，验证该账户及所对应的密码是否正确。如果正确，认证过程结果，允许用户登录，否则拒绝用户登录。

随着计算机网络的迅速发展和应用系统的不断增加，大多数用户不得不通过网络远程登录主机系统，用户和主机系统之间就必须在网上进行密码认证。而因特网上泛滥的网络监听工具(如 Sniffer 等)可以非常容易地监听到网络上传递的各类明文信息，包括 FTP、Telnet 和 POP3 等网络服务的账户及密码。如果在网络上传送的账户和密码没有经过加密处理，就很容易被窃取，这是一种非常不安全的密码认证方式。

入侵者经常通过窃取密码数据库或监听网络信息，获得合法用户的账户及密码，然后入侵网络计算机系统，进行非法攻击和违法活动。为此，就密码的安全使用来说，计算机系统应该具备下列安全性。

(1) 入侵者即使取得储存在系统中的密码也无法达到登录的目的。这需要在密码认证的基础上再增加其他的认证方式，如地址认证。

(2) 通过监听网络上传送的信息而获得的密码是不能用的。最有效的方式是数据加密。

(3) 计算机系统必须能够发现并防止各类密码尝试攻击。可使用密码安全策略。

4.2.2 密码认证的安全性

由于密码被窃听、盗用和入侵等问题，密码认证的安全性问题多年来一直是人们讨论的焦点，密码认证的操作方式直接影响着计算机系统的安全性。

早在 1974 年，Purdy 就提到为了保护密码的安全，绝对不能以明文的方式储存密码，提出将密码以单向函数 $y=f(x)$ 转换后，以加密的方式将密码与账户资料存放在一个验证表中。单向函数应具有下列特性。

(1) 知道 x 可以很容易计算出 y。

(2) 知道 y 要算出 x，在计算上是不可行的。

此后便有很多关于密码认证的方法被提出，这些方法有的着重在讨论加密的运算，有的强调加密和解密的效率，但其目的都是为了保护密码数据库，即使密码数据库文件被别人窃取，

要想破解出密码的明文也是非常困难的。例如,在 UNIX 系统中,为了防止密码泄露,对密码进行 Hash 函数变换后再存放在/etc/passwd 或/etc/shadow 系统密码文件中。

但是,在这种方式中却忽略了重放攻击。当入侵者从网络上窃听到合法用户的账户和密码,然后进行重放攻击,主机系统将无法判断密码认证请求的信息是来自合法用户还是重放攻击。只要密码认证的请求信息被复制重放,计算机系统就会处于不安全的状态。所谓"重放攻击(Replay Attacks)",也称为"新鲜性攻击(Freshness Attacks)",即攻击者通过重放消息或消息片段达到对目标主机进行欺骗的攻击行为,其主要用于破坏认证的正确性。重放攻击是攻击行为中危害较为严重的一种。例如客户 C 通过签名授权银行 B 转账给客户 A,如果攻击者 P 窃听到该消息,并在稍后重放该消息,银行将认为客户需要进行两次转账,从而使客户账户遭受损失。

使用一次性密码(即"一次一密")技术可以防止重放攻击的发生,这相当于用户随身携带一个密码本,按照与目标主机约定好的次序使用这些密码,并且每一个密钥只使用一次,当密码全部用完后再向系统管理员申请新的密码本。S/Key 认证系统就是基于这种思想的一次性密码认证系统。在 S/Key 认证系统中,用户每一次登录系统所用的密码都是不一样的,攻击者通过窃听得到的密码无法用于下一次认证,这样 S/Key 认证系统很好地防止了密码重放攻击。相对于可重放的密码认证系统,S/Key 认证系统具有很好的安全性,而且符合安全领域的发展趋势。

Lamport 算法是另一种防止重放攻击的有效方法。Lamport 算法使用安全单向 Hash 函数 $y=F(x)$的动态密码认证方法,使用者每一次登录的密码都不同。即用安全单向函数 $y=F(x)$对用户的密码明文经过多次迭代运算,产生一系列一次性口令,即

$$PW_i = F^{N+1-i}(password), \quad i = 1,2,3,\cdots,N$$

根据以上函数关系,可以计算出第一个一次性密码为 PW_1,这时用户的密码明文经过了 N 次迭代运算;第二个一次性密码为 PW_2,这时用户的密码明文经过 $N-1$ 次迭代运算。依此类推,得到所有的一次性密码列表。

把第一个一次性密码 PW_1 和迭代次数 N 存放到服务器上。当用户通过网络对服务器进行访问时,服务器把迭代次数 $m(m<N)$发送给用户端,用户端根据迭代次数 m 计算出下一个一次性密码 PW_{m+1},并通过网络发送到服务器。服务器经过一次单向 Hash 函数运算,把结果和保留在服务器上的用户密码进行比较,如果两者相等,通过认证,允许访问,否则拒绝访问。如果成功进行了访问,则用刚传过来的一次性密码 PW_{m+1} 来替换掉服务器端存储的用户密码 PW_m,并把迭代次数 m 减 1。

这样攻击者即使从网络上窃取了用户密码,也无法计算出下一个正确的用户密码,因为单向函数是不可逆的,知道函数输出值,无法计算得到函数的输入值。这个方法必须依赖 $F(x)$ 是一个安全的函数,也就是 $F(x)$函数不可被破解,而且在系统运行中不能更换 $F(x)$函数。

一次性口令有其安全的地方,但在实际应用中很不方便。如密码更改问题、初始化问题等。本次密码列表中的密码被全部使用后,用户必须向系统管理员重新申请新的密码和迭代函数。

4.2.3 密码认证中的其他问题

通过用户账户和密码进行认证是操作系统和应用程序主要采用的身份认证方式。但是,在实际应用中,大量用户都不可能使用一次性密码,而是使用大量的弱密码。大量弱密

码的存在，增加了网络的不安全因素。下面通过对常用密码攻击手段的介绍，来说明弱密码存在的严重安全威胁。

1. 社会工程学

社会工程学(Social Engineering)是一种通过对受害者心理弱点、本能反应、好奇心、信任和贪婪等心理陷阱进行的诸如欺骗、伤害等危害手段，取得自身利益的手法，近年来已成迅速上升甚至滥用的趋势。

运用社会工程学进行网络攻击有很多方法，并且许多方法并不需要较强的技术支持，攻击者只需要懂得如何利用人的弱点(如轻信、健忘、胆小和贪婪等)就可以轻易地潜入防护最严密的网络系统。例如，“网络钓鱼”就是近来社会工程学的代表应用，在“网络钓鱼”中利用欺骗性的电子邮件和伪造的网络站点来进行诈骗，专门骗取电子邮件接收者身份证号、银行密码和信用卡卡号等个人信息，然后再利用这些信息从事非法行为。

2. 按键记录软件

按键记录软件是一种间谍软件，它以木马方式植入到用户的计算机后，可以偷偷地记录下用户的每次按键动作，并按预定的计划把收集到的信息通过电子邮件等方式发送出去。例如，如果用户在运行有按键记录软件的计算机上登录了网上银行，那么用户的账户和密码无疑就暴露给了犯罪分子，后果可想而知。

3. 搭线窃听

攻击者通过窃听网络数据，如果密码使用明文传输，可被非法获取。目前，在 IP 网络中 Telnet、FTP 和 HTTP 等大量的通信协议用明文传输密码，这意味着在客户端和服务器端之间传输的所有信息(其中包括明文密码和用户数据)都有可能被窃取。

4. 字典攻击

大多数用户习惯于选取用户的姓名、生日及相关信息等容易记忆的信息作为密码，由此产生的密码容易被攻击者猜到。攻击者可以把所有用户可能选取的密码列举出来生成一个文件，这样的文件被称为“字典”。当攻击者得到了一些与密码有关的可验证信息后，就可以结合字典进行一系列的运算，来猜测用户可能的密码，并利用得到的信息来验证猜测的正确性。为此，许多系统要求用户在密码中使用特殊字符，以增加密码的安全性。

5. 暴力破解

暴力破解也称为“蛮力破解”或“穷举攻击”，是一种特殊的字典攻击。在暴力破解中所使用的字典是字符串的全集，对可能存在的所有组合进行猜测，直到得到正确的信息为止。从理论上讲，只要计算机的处理能力足够强、时长允许，所有密码都是可以被破解的。如果用户的密码较短，可以在较短的时间内被穷举出来。所以许多系统建议用户使用长密码。

6. 窥探

窥探是攻击者利用与被攻击系统接近的机会，安装监视设备或亲自窥探合法用户输入的账户和密码。窥探还包括攻击者在用户计算机中植入的木马。

7. 垃圾搜索

垃圾搜索是攻击者通过搜索被攻击者的废弃物(如硬盘、U 盘和光盘等)，得到与攻击系统有关的信息。如果用户将账户和密码写在纸上，这些记录用户私密信息的纸张没有被安全保管，则很有可能成为攻击者的搜索对象。

4.3 基于地址的身份认证

在计算机网络中,除密码外,地址是应用较为广泛的一种身份认证方式。基于地址的身份认证的优点是不需要使用密码来验证身份,可以防止密码窃听现象的发生。

4.3.1 地址与身份认证

在计算机网络出现的早期,由于计算机网络的规模比较小,应用比较单一,所以网络地址很自然地成为彼此之间建立信任关系的主要依据。例如 UNIX 操作系统中的 rlogin、rsh 和 rcp 等一系列远程计算工具都是依据对方的地址来判断身份的。

Internet 中主机之间的通信是利用 IP 地址来认证的,所以在 Internet 中主机的唯一身份就是 IP 地址。一方面通过 IP 地址的规范管理,确保 Internet 的有序运行和发展;另一方面通过对 IP 地址的控制,可以限制主机之间的通信。将 IP 地址作为身份认证的依据,在理论上是可行的,但在实际应用中是不可靠的。IP 地址可以用于广义的身份认证,例如在发布 Web 网站时,可以限制只允许某一个 IP 地址段的用户能够访问,在进行防火墙的配置时可以限制某些 IP 地址段的用户无法访问外部网络等。但是,由于 IP 地址与系统资源之间,以及 IP 地址与用户或设备之间没有确定的一一对应关系,而认证的目的是为授权提供身份的真实性,只有通过认证的用户才可以访问系统资源,所以将 IP 地址用于身份认证是不安全的,也是不可行的。

计算机网络中的地址可以分为逻辑地址和物理地址两大类,其中 IP 地址属于逻辑地址,而设备的硬件地址(如网卡的 MAC 地址等)属于物理地址。凡是工作于 OSI 七层模型的第二层(数据链路层)的设备都拥有一个全球唯一的物理地址,这个地址就是 MAC 地址。由于 MAC 地址的唯一性,所以在理想条件下可以利用 MAC 地址进行身份认证。例如,在 Cisco 交换机上可以通过以下命令进行主机 MAC 地址与交换机端口的绑定。

Switch(config)#int fa0/1 (进入交换机的 Fa0/1 端口)

Switch(config-if)#switchport port-security (启动端口安全模式)

Switch(config-if)#switchport port-security maximum 1 (设置该端口的最大可用地址为 1)

Switch(config-if)# switchport port-security *mac-address* (设置该端口绑定的 MAC 地址)

通过以上设置,当交换机的 Fa0/1 端口接收到通信请求时,交换机首先要检查收到的数据帧的 MAC 地址与该端口已绑定的 MAC 地址是否相同。如果相同认证通过,允许进行通信,否则认证失败,拒绝进行通信。

通过前面的例子可以看出,物理地址在身份认证中似乎是可靠性。但事实上并非如此,不但今天的主流操作系统(如 Windows 2000/XP/2003/Vista、Linux 等)可以直接修改网卡的 MAC 地址,而且近一段时间在网络中泛滥的 ARP 欺骗病毒可以伪造任何一个 MAC 地址进行攻击。所以,基于地址的认证方式其可靠程度越来越低。

4.3.2 智能卡认证

智能卡(Smart Card)也称 IC 卡,是由一个或多个集成电路芯片(包括固化在芯片中的软件)组成的设备,可以安全地存储密钥、证书和用户数据等敏感信息,防止硬件级别的窜

改。智能卡芯片在很多应用中可以独立完成加密、解密、身份认证和数字签名等对安全较为敏感的计算任务，从而能够提高应用系统抗病毒攻击及防止敏感信息的泄漏。

智能卡具有硬件加密功能，所以安全性较高。每个用户持有一张智能卡，智能卡存储用户个人的秘密信息，同时在验证服务器中也存放该秘密信息。进行认证时，用户输入 PIN（个人身份识别码），智能卡认证 PIN 成功后，即可读出智能卡中的秘密信息，进而利用该秘密信息与主机之间进行认证。

智能卡认证是基于 what you have 的手段，通过智能卡硬件不可复制来保证用户身份不会被仿冒。基于智能卡的认证方式是一种双因素的认证方式，首先认证 PIN（可以理解为具有唯一性的地址），当 PIN 通过认证后再认证智能卡。所以，除非 PIN 和智能卡被同时窃取，否则用户不会被冒充。

本节提到了“双因素认证”的概念。所谓双因素身份认证，简单地讲是指在身份认证过程中至少提供两个认证因素，如“密码＋PIN”等。双因素认证与利用 ATM（自动柜员机）取款很相似：用户必须持银行卡（认证设备），再输入密码，才能提取其账户中的款项。双因素认证提供了身份认证的可靠性。

4.4 生物特征身份认证

前面分别介绍了基于密码的身份认证和基于地址的身份认证，从技术发展来看，这两种传统的认证方式都存在缺陷，取而代之的将是目前正在兴起的生物特征的认证方式。

4.4.1 生物特征认证的概念

生物特征认证又称为“生物特征识别”，是指通过计算机利用人体固有的生理特征或行为特征鉴别个人身份。在信息安全领域，推动基于生物特征认证的主要动力来自于基于密码认证的不安全性，即利用生物特征认证来替代密码认证。

人的生理特征与生俱来，一般是先天性的。行为特征则是习惯养成，多为后天形成。生理和行为特征统称为生物特征。常用的生物特征包括脸像、虹膜、指纹、声音和笔迹等。同时，随着现代生物技术的发展，尤其对人类基因研究的重大突破，研究人员认为 DNA 识别技术将是未来生物识别技术的又一个发展方向。满足以下条件的生物特征才可以用来作为进行身份认证的依据。

- 普遍性。每一个人都应该具有这一特征。
- 唯一性。每一个人在这一特征上有不同的表现。
- 稳定性。这一特征不会随着年龄的增长和生活环境的改变而改变。
- 易采集性。这一特征应该便于采集和保存。
- 可接受性。人们能够接受这种生物识别方式。

生物特征认证的核心在于如何获取这些特征，并将其转换为数字形式存储在计算机中，并利用可靠的匹配算法来完成验证与识别个人身份的过程。生物识别系统包括采集、解码、比对和匹配几个处理过程。

与传统的密码、地址等认证方式相比，生物特征认证具有依附于人体、不易伪造和不易模仿等特点和优势，已成为身份认证技术中发展最快、应用前景最好的一项关键技术。国际

民用航空组织已建议187个成员将脸像、虹膜或指纹等生物特征放入护照。与此同时，全球生物特征技术产品也迅速发展起来。

4.4.2 指纹认证

利用人的生物特征可以实现“以人识人”，其中指纹是人的生物特征中一种重要的表现形式，具有“人人不同”和“终身不变”的特征，以及附属于人的身体的便利性和不可伪造的安全性。

指纹识别技术也称为“指纹认证技术”，早在1858年印度的William Hershel爵士就使用指纹和掌纹作为合同签名的一种形式。目前，在全球范围内都建立了指纹鉴定机构及罪犯指纹数据库，我国早在20世纪80年代的重点人口管理中就开始采集具有犯罪前科的重点人口的指纹，并相继建立了全国范围内联网的指纹比对数据库。早期的指纹认证主要用于司法鉴定，现在已广泛应用于门禁系统、考勤、部分笔记本电脑和移动存储设备。认证技术在不断成熟，应用范围也在不断拓宽。

指纹认证的特点如下。

(1) 独特性。19世纪末，英国学者亨利提出了基于指纹特征进行认证的原理和方法。根据亨利的理论，一般人的指纹在出生后的9个月便成形，并终生不会改变；每一个指纹都有70～90个基本特征点。另外，据最近的一项统计，在全世界60多亿人口中，没有两个人的指纹是完全相同的。因此，指纹具有高度的不可重复性，如图4-2所示。





图4-2 不同的指纹形状

(2) 稳定性。指纹纹脊的样式终端不变。指纹不会随着人的年龄、健康程度的变化而发生变化。

(3) 方便性。目前已建有标准化的指纹样本库，以方便指纹认证系统的开发。同时，在指纹识别系统中用于指纹采集的硬件设备也较容易实现。

如图4-3所示，指纹识别的过程包括两个子过程：指纹注册过程和指纹比对过程。

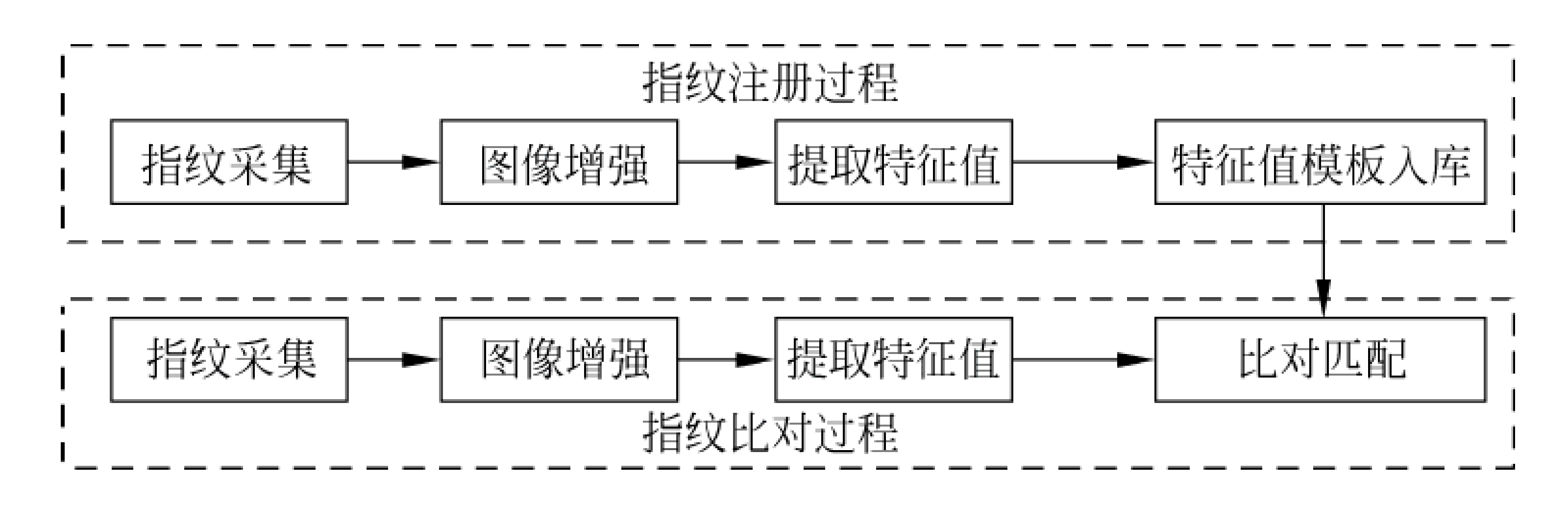


图4-3 指纹识别系统的组成

① 指纹采集。通过指纹传感器获取人的指纹图像数据，其本质是指纹成像。指纹采集大都通过各种采集仪，可分为光学和 COMS 两类，其中光学采集仪采集图像失真小，但成本较高；而 COMS 采集仪成本低，但图像质量较差。

② 图像增强。根据某种算法，对采集到的指纹图案进行效果增强，以利于后续对指纹特征值的提取。

③ 提取特征值。对指纹图案上的特征信息进行选择(如图 4-4 所示)、编码和形成二进制数据的过程。

④ 特征值模板入库。根据指纹算法的数据结构，即特征值模板，对提取的指纹特征值进行结构化并保存起来。

⑤ 比对匹配。把当前取得的指纹特征值集合与已存储的指纹特征值模板进行匹配的过程。


图 4-4 指纹图案信息的选择

4.4.3 虹膜认证

作为生物特征认证的依据，指纹的应用已经比较广泛，然而指纹识别易受脱皮、出汗和干燥等外界条件的影响，并且这种接触式的识别方法要求用户直接接触公用的传感器，给使用者带来了不便。例如，在非典型性肺炎、禽流感等疾病的传播期间，如果使用这种直接接触式的认证就会存在一定困难。为此，非接触式的生物特征认证将成为身份认证发展的必然趋势。与脸像、声音等其他非接触式的身份鉴别方法相比，虹膜以其更高的准确性、可采集性和不可伪造性，成为目前身份认证研究和应用的热点。

基于虹膜的身份认证要求对被认证者的虹膜特征进行现场实时采集，用户在使用虹膜进行身份认证时无需输入 ID 号等标志信息。

1993 年英国剑桥大学计算机实验室的 J. G. Daugman 率先研制出基于 Gabor 变换的虹膜识别算法，实现了一个高性能的虹膜识别系统。1994 年澳大利亚的 R. P. Wildes 研制出基于图像配准技术的虹膜识别系统。1997 年，W. W. Boles 等人用小波变换进行虹膜的识别。虹膜身份识别技术涉及数学、信号处理、模式识别、图像处理等多个领域，是当今计算机应用领域的研究课题之一。

从理论上讲，虹膜认证是基于生物特征的认证方式中最好的一种认证方式。虹膜(眼睛中的彩色部分)是眼球中包围瞳孔的部分(如图 4-5 所示)，上面布满极其复杂的锯齿网络状花纹，而每个人虹膜的花纹都是不同的。虹膜识别技术就是应用计算机对虹膜花纹特征进行量化数据分析，用以确认被识别者的真实身份。

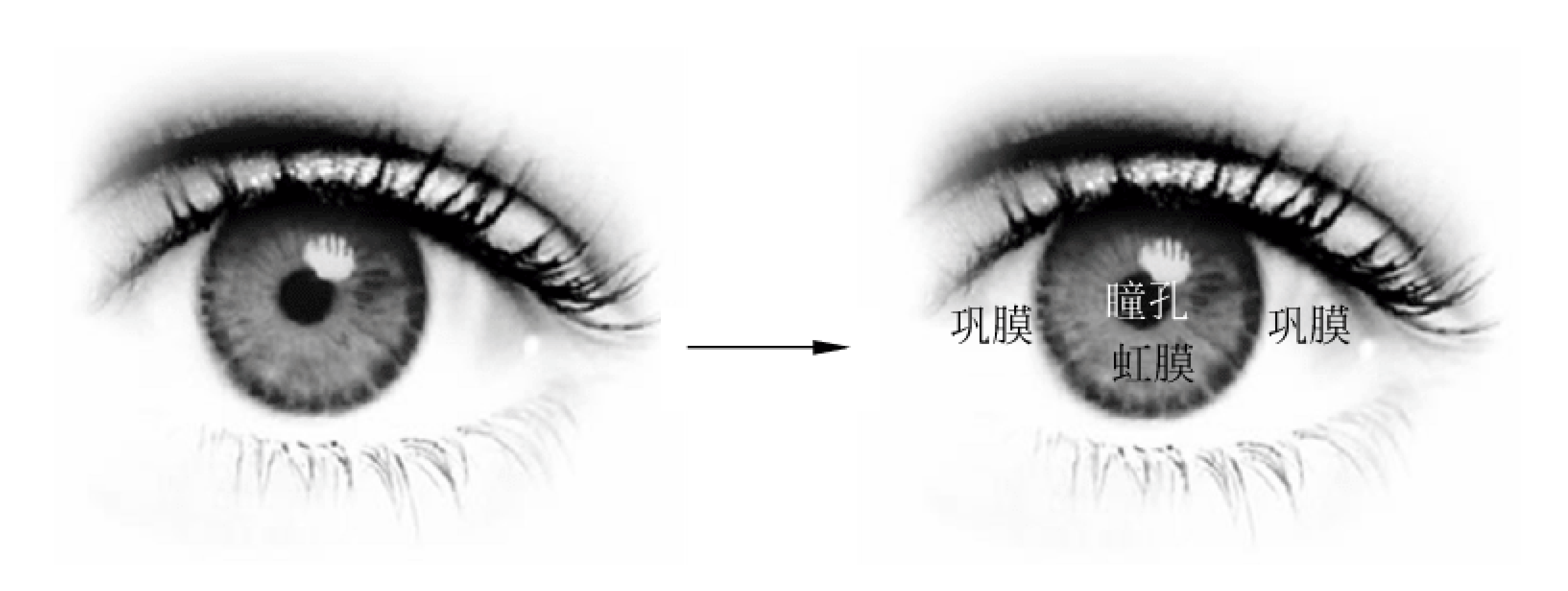


图 4-5 虹膜在眼球中的位置

每一个人的虹膜具有随机的细节特征和纹理图像。这些特征在人的一生中保持相对的稳定性,不易改变。据统计,到目前为止,虹膜认证的错误率在所有的生物特征识别中是最低的(相同纹理的虹膜出现的概率是 10^{-46})。所以虹膜识别技术在国际上得到广泛的关注,有很好的应用前景。

如图 4-6 所示,一个虹膜识别系统一般由 4 部分组成:虹膜图像的采集、预处理、特征提取及模式匹配。

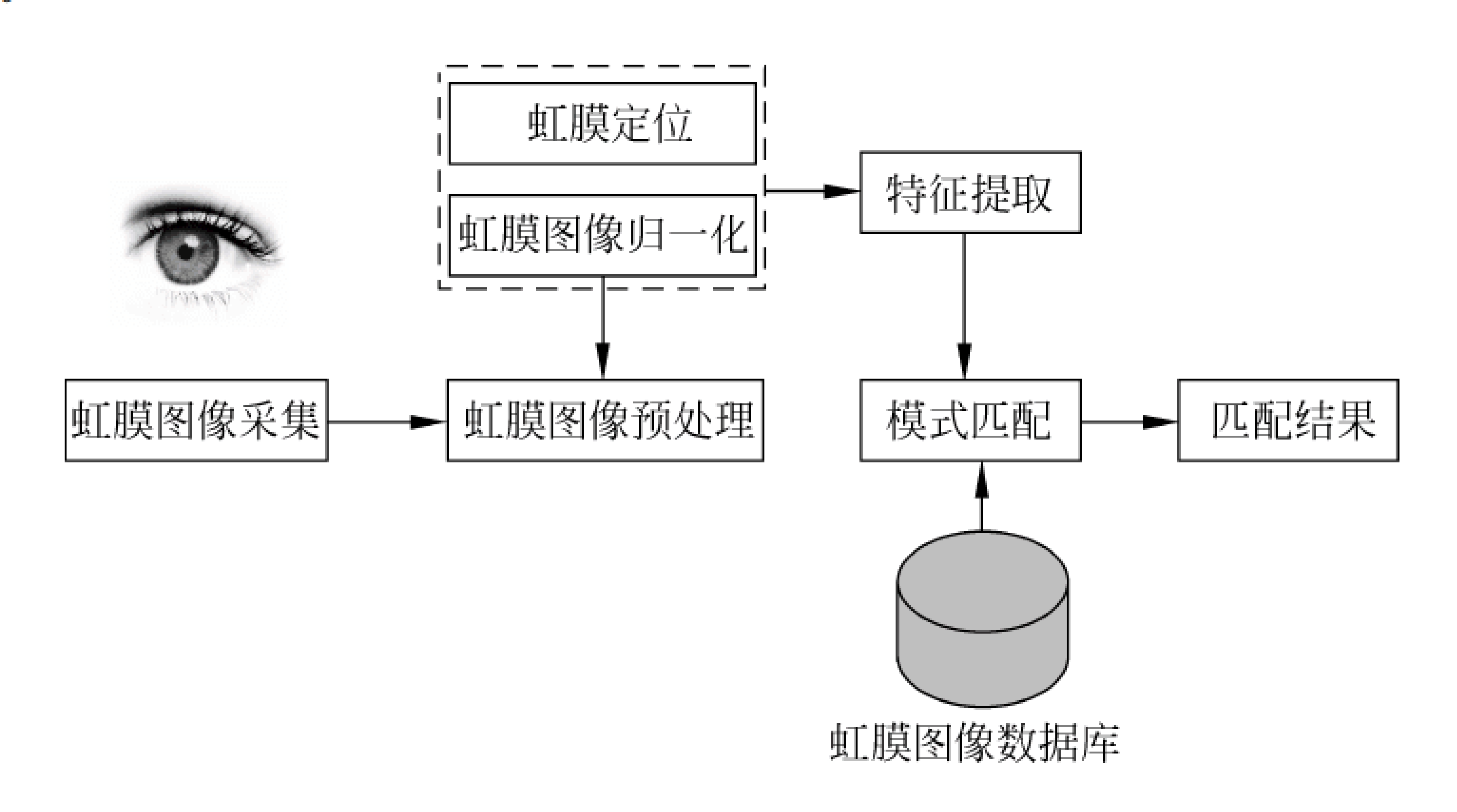


图 4-6　虹膜识别系统的组成

① 虹膜图像采集。虹膜图像采集是虹膜识别系统中一个重要的且困难的步骤。因为虹膜尺寸比较小且颜色较暗,所以用普通的照相机来获取质量好的虹膜图像是比较困难的,必须使用专门的采集设备。

② 虹膜图像的预处理。这一操作分为虹膜定位和虹膜图像的归一化两个步骤。其中,虹膜定位就是要找出瞳孔与虹膜之间(内边界)、虹膜与巩膜之间(外边界)的两个边界,再通过相关的算法对获得的虹膜图像进行边缘检测。对虹膜图像进行归一化是由于光照强度及虹膜震颤的变化,瞳孔的大小会发生变化,而且在虹膜纹理中发生的弹性变形也会影响虹膜模式匹配。因此,为了实现精确的匹配,必须对定位后的虹膜图像进行归一化,补偿大小和瞳孔缩放引起的变异。

③ 虹膜纹理的特征提取。采用转换算法将虹膜的可视特征转换成为固定字节长度的虹膜代码。

④ 模式匹配。识别系统将生成的代码与代码数据库中的虹膜代码逐一比较,当相似率超过某一个预设置值时,系统判定检测者的身份与某一个样本相符,否则系统将认为检测者的身份与该样本不相符,接着进入下一轮的比较。

以上过程,虽然介绍起来比较简单,但实现起来非常复杂,需要解决大量的技术问题。

4.5　零知识证明身份认证

在前面介绍的身份认证过程中,一般验证者在收到证明者提供的认证账户和密码后,在数据库中进行核对,如果在验证者的数据库中找到了证明者提供的账户和密码,该认证通过,否则认证失败。在这一认证过程中,验证者必须事先知道证明者的账户和密码,这显然会带来不安全因素。那么,能否实现在验证者不需要知道证明者任何信息(包括用户账户和

密码)的情况下就能够完成对证明者的身份认证呢?零知识证明身份认证就可以实现这一功能。

4.5.1 零知识证明身份认证的概念

零知识证明(zero-knowledge proof)是在20世纪80年代初出现的一种身份认证技术。零知识证明是指证明者能够在不向验证者提供任何有用信息的情况下,使验证者相信某个论断是正确的。

零知识证明实质上是一种涉及两方或多方的协议,即两方或多方完成一项任务所需采取的一系列步骤。证明者向验证者证明并使验证者相信自己知道某一消息或拥有某一物品,但证明过程不需要(也不能够)向验证者泄漏。零知识证明分为交互式零知识证明和非交互式零知识证明两种类型。下面给出一个零知识证明的例子。

用户A要向用户B证明自己是某一间房子的主人,即A要向B证明自己能够正常进入该房间。现在假设该房间只能用钥匙打开锁后进入,而其他任何方法都打不开。这时有两种办法:一种方式是A把钥匙交给B,B拿着这把钥匙打开该房间的锁,如果B能够打开则证明A是该房间的主人;另一种方式是B确定该房间内有一个物品,只要A用自己的钥匙打开该房间后,将该物品拿出来出示给B,从而证明A是该房间的主人。其中,后一种方式属于零知识证明。虽然两种方式都证明了用户A是该房子的主人,但在后一种方式中用户B始终没有得到用户A的任何信息(包括没有拿到用户A的钥匙),从而可以避免用户A的信息(钥匙)被泄露。

下面,结合公开密钥算法来介绍零知识证明的特点。用户A拥有用户B的公钥,现在用户B需要向A证明自己的身份是真实的。同样有两种证明的方法:一种方式是用户B把自己的私钥交给A,A用这个私钥对某个数据进行加密操作,然后将加密后的密文用B的公钥来解密,如果能够成功解密,则证明用户B的身份是真实的。另一种方式是用户A给出一个随机值,B用自己的私钥对该随机值进行加密操作,然后把加密后的数据交给A。A用B的公钥进行解密操作,如果能够得到原来的随机值,则证明用户B的身份是真实的。其中,后一种方式属于零知识证明,在整个过程中B没有向A提供自己的私钥。

零知识证明当中验证者B选择随机数,证明者A根据随机数出示不同的证明。一方面A不能欺骗B,因为他的随机数要求使用其私钥运算;另一方面B也不能伪装A来欺骗C,因为随机数将由C选择,B不能重发他与A之间的验证信息。证明者欺骗验证者的概率随着随机数选择的位数和验证次数的增多而减少。

4.5.2 交互式零知识证明

零知识证明协议可定义为证明者(Prover,简称P)和验证者(Verifier,简称V)。交互式零知识证明是由这样一组协议确定的:在零知识证明过程结束后,P只告诉V关于某一个断言成立的信息,而V不能从交互式证明协议中获得其他任何信息。即使在协议中使用欺骗手段,V也不可能揭露其信息。这一概念其实就是零知识证明的定义。

如果一个交互式证明协议满足以下3点,就称此协议为一个零知识交互式证明协议。

- 完备性。如果P的声称是真的,则V以绝对优势的概率接受P的结论。
- 有效性。如果P的声称是假的,则V也以绝对优势的概率拒绝P的结论。

- 零知识性。无论 V 采取任何手段,当 P 的声称是真的,且 P 不违背协议时,V 除了接受 P 的结论以外,得不到其他额外的信息。

简单地讲,交互式零知识证明就是为了证明 P 知道一些事实,希望验证者 V 相信他知道的这些事实而进行的交互。为了安全起见,交互式零知识证明是由规定轮数组成的一个“挑战/应答”协议。通常每一轮由 V 挑战和 P 应答组成。在规定的协议结束时,V 根据 P 是否成功地回答了所有挑战来决定是否接受 P 的证明。

前面介绍的用户 A 要向用户 B 证明自己是某一间房子的主人的例子,便是一个交互式零知识证明的示例。在这一认证过程中,只进行了一轮挑战和应答。出于安全考虑,还可以通过其他方式再增加几轮挑战和应答。

4.5.3 非交互式零知识证明

在交互式零知识证明过程中,证明者和验证者之间必须进行交互。20 世纪 80 年代末,出现了“非交互式零知识证明”的概念。在非交互式零知识证明过程中,通信双方不需要进行任何交互,从而任何人都可以对 P 公开的消息进行验证。

在非交互式零知识证明中,证明者 P 公布一些不包括他本人任何信息的秘密消息,却能够让任何人相信这个秘密消息。在这一过程(其实是一组协议)中,起关键作用的因素是一个单向 Hash 函数。如果 P 要进行欺骗,他必须能够知道这个 Hash 函数的输出值。但事实上由于他不知道这个单向 Hash 函数的具体算法,所以他无法实施欺骗。也就是说,这个单向 Hash 函数在协议中是 V 的代替者。

目前非交互式零知识证明的实现可采用多种算法,具体算法不再介绍,读者可参阅相关的资料。

4.6 身份认证协议

计算机网络中的身份认证协议是指对参与通信的主体(如用户、计算机等)之间提供安全认证的协议。网络环境中的身份认证协议及系统,在网络安全中占据十分重要的位置,对于网络应用的安全有着非常重要的作用。本节介绍几种典型的身份认证协议。

4.6.1 Kerberos 协议

Kerberos 协议是麻省理工学院开发的基于 TCP/IP 网络设计的可信第三方认证协议,它是目前分布式网络计算环境中应用最为广泛的认证协议。

1. Kerberos 协议简介

Kerberos 是为基于 TCP/IP 的 Internet 和 Intranet 设计的安全认证协议,它工作在 Client/Server 模式下,以可信赖的第三方 KDC(密钥分配中心)实现用户身份认证。在认证过程中,Kerberos 使用对称密钥加密算法,提供了计算机网络中通信双方之间的身份认证。

Kerberos 设计的目的是解决在分布网络环境中用户访问网络资源时的安全问题。Kerberos 的安全性不依赖于用户端计算机或者要访问的主机(如服务器),而是依赖于 KDC。Kerberos 协议中每次通信过程都有三个通信参与方:需要验证身份的通信双方和一个双方都信任的第三方 KDC。将发起认证服务的一方称为客户端,客户端需要访问的对

象称为服务器端。在 Kerberos 中，客户端是通过向服务器端提交自己的“凭据(Ticket)”来证明自己的身份，该凭据是由 KDC 专门为客户端和服务器端在某一阶段内通信而生成的。Kerberos 保存一个它的客户端及密钥的数据库，这些密钥是 KDC 与客户端之间共享的，是不能被第三方知道的。

由于 Kerberos 是基于对称加密来实现认证的，这就涉及到加密密钥对的产生和管理问题。在 Kerberos 中会对每一个用户分配一个密钥对，如果网络中存在 N 个用户，则 Kerberos 系统会保存和维护 N 个密钥对。同时，在 Kerberos 系统中只要求使用对称密码，而没有对具体算法和标准作限定，这样便于 Kerberos 协议的推广和应用。

Kerberos 已广泛应用于 Internet 和 Intranet 服务的安全访问，具有高度的安全性、可靠性、透明性和可伸缩性等优点。目前许多远程访问认证服务系统都支持 Kerberos 认证协议，如微软公司的 EAP(可扩展认证协议)、Cisco 公司的 TACACS(终端访问控制器访问控制系统)以及远程用户认证拨号系统(RADIUS)等，同时 Windows 2000/2003 操作系统也将 Kerberos 集成作为本地认证协议。

目前广泛使用的 Kerberos 的版本是第 4 版(v4)和第 5 版(v5)，其中 Kerberos v5 弥补了 v4 中存在的一些安全漏洞。Kerberos v5 已成为 Internet 标准(RFC 1510)。

2. Kerberos 系统的组成

一个完整的 Kerberos 系统主要由以下几个部分组成。

(1) 用户端(Client)。需要提供身份认证的一方，有可能是用户账户，也有可能是设备的地址。如果是用户账户，用户端的密钥是通过账户对应的密码得出的。

(2) 服务器端(Server)。为用户端提供资源的服务器，当用户访问这些资源时需要进行身份认证。只有当认证通过后才允许访问。该服务器一般也称为资源服务器。

(3) 密钥分配中心(Key Distribution Center，KDC)。Kerberos 使用了一个可依赖的第三方 KDC 为需要认证的用户提供对称密钥，如 K_A、K_B 和 K_C 等。为每一个用户提供的对称密钥只有该用户和 KDC 知道。另外，在 KDC 中还有一个主密钥 K_{KDC}，这个密钥是在 KDC 内部使用的密钥。由于 KDC 在 Kerberos 系统中的重要性，所以 KDC 的安全在很大程度上决定了 Kerberos 系统的安全。在 Kerberos 系统中设置了两个服务器：认证服务器和票据分配服务器。

(4) 认证服务器(Authentication Server，AS)。在 KDC 中，由 AS 为用户提供身份认证，AS 将用户的密码保存在 KDC 的数据库中。当用户需要进行身份认证时，AS 在收到密钥后与数据库中的密码进行比对，如果比对通过，AS 将向用户发放一个票据。用户根据该票据去访问资源服务器上的资源。

(5) 票据分配服务器(Ticket Granting Server，TGS)。在用户访问服务器端的资源时，为了避免 AS 每次都要向用户发放票据，所以在 KDC 中提供了 TGS。TGS 的作用是向已经通过 AS 认证的用户发放用于获取资源服务器上提供的服务的票据。当用户要访问资源服务器上的资源时，AS 发放一个“票据许可票据(Tickettgs)”，用户会保存该票据。以后，当用户再次访问资源服务器上的资源时，只需要向 TGS 出示 Tichettgs，TGS 会向用户发放一个“服务许可票据(Tickettv)”，用户根据 Tickettv 在资源服务器上访问所需要的资源。

(6) 票据。票据的作用是在身份认证服务器(AS 和 TGS)与资源服务器之间安全地传

递用户的身份信息,同时也将身份认证服务器对用户的信任信息转发给资源服务器。在票据中包括服务器名称、用户的名称、用户的地址、时间标记、生命周期以及一个随机的会话密钥。票据在服务器之间传递时都是加密的。

(7) 时间戳。在计算机网络系统的安全管理中经常要用到时间戳的概念。当用户获得一个访问资源服务器的票据时,在票据中包含一个时间戳,指明票据发出的时期、时间以及它的生命周期。通过时间戳,用户可知道票据的有效性。需要说明的是,当时间戳用于认证时,不同设备之间的时钟需要进行精确同步,或提供必要的时钟偏差。在 Kerberos 中,时钟偏差被设置为 5 分钟。

另外,还有保证票据、密码等信息安全传输中所需要的密钥。

3. Kerberos 的基本认证过程

如图 4-7 所示,下面介绍 Kerberos 的基本认证过程。

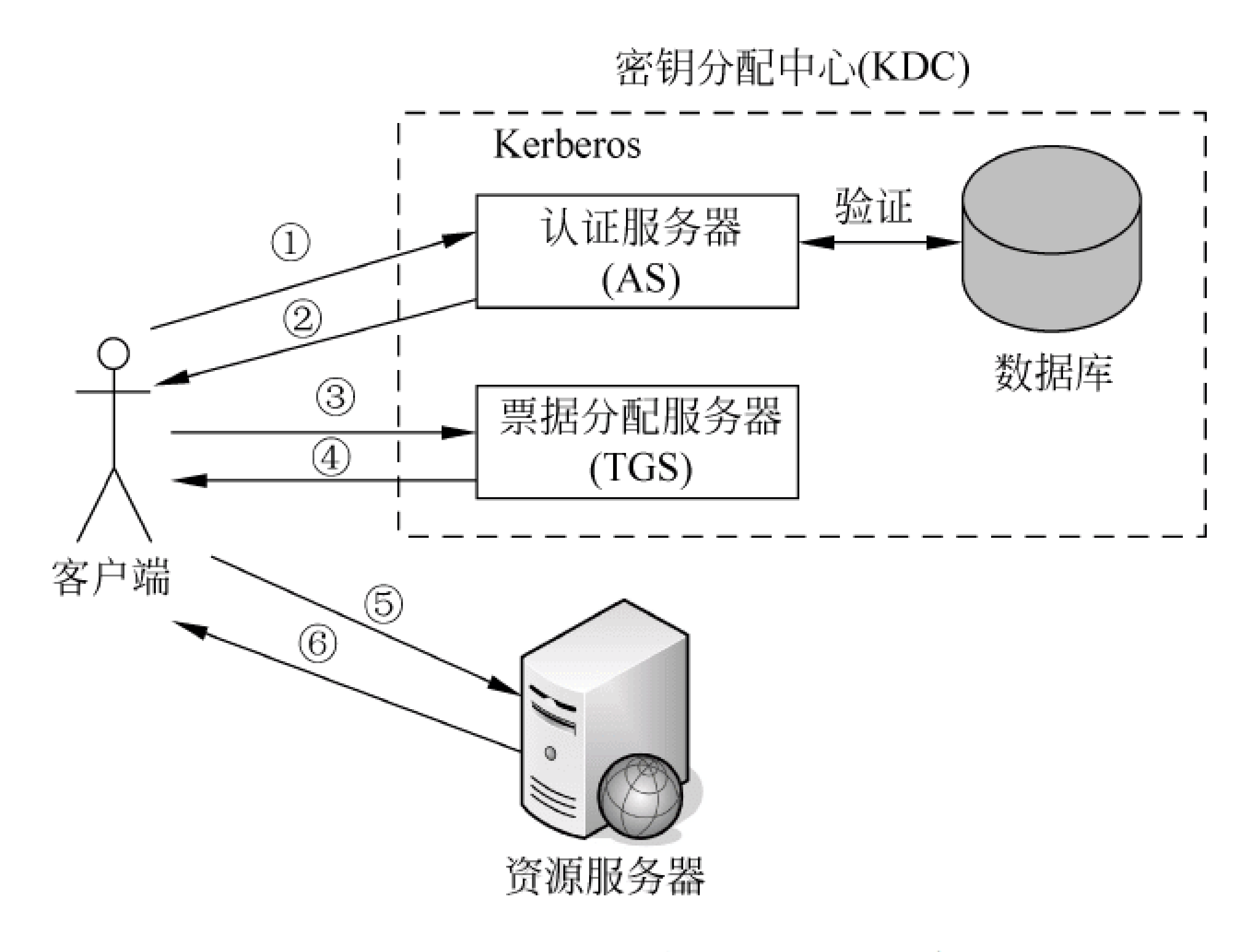


图 4-7　Kerberos 系统认证过程示意图

① 客户端在计算机上向 AS 发送一个包含客户端名称(用户名)、资源服务器名称的认证信息。

② 首先,AS 验证客户端的真实性后,随机生成一个加密密钥作为下一阶段客户端与 TGS 通信时使用的会话密钥。接着,AS 构造一个包含客户端、会话密钥及开始和失效时间等信息的"票据许可票据",并将该票据用 TGS 的密钥进行加密。然后,AS 将新的会话密钥用客户端的密钥 K_C 加密(对称加密),并与"票据许可票据"一起发送给客户端。最后,客户端计算机利用用户输入的密码生成密钥 K_C,并用该密钥 K_C 解密收到的信息,得到所需要的会话密钥 $K_{C,tgs}$ 以及"票据许可票据",并利用时间戳确保"票据许可票据"是最新的。

③ 客户端向 TGS 发送一个包含访问 TGS 时使用的"票据许可票据"、需要访问的资源服务器名称、客户端名称及客户端密钥 K_C 的信息,该信息使用②中得到的会话密钥进行加密,以防止信息在发给 TGS 的过程中被篡改。

④ TGS 用自己的密钥验证"票据许可票据"后,获得在②中构造的会话密钥 $K_{C,tgs}$ 和客户端要访问的资源服务器的名称,并从数据库中获得资源服务器的密钥 K_S 后随机生成客户端与资源服务器之间通信时使用的会话密钥和"服务许可票据"。TGS 将客户端与资源

服务器之间使用的新的会话密钥用从“票据许可票据”中获得的会话密钥 $K_{C,tgs}$ 加密后与新的“服务许可票据”一起发给客户端。

⑤和⑥ 客户端向资源服务器发送包含有认证者身份和“服务许可票据”的信息，资源服务器通过解密获得客户端的信息，完成认证。

4.6.2 SSL 协议

SSL(Secure Socket Layer，安全套接字层)协议最初是由 Netscape Communication 公司设计开发的安全认证协议，也是国际上最早应用于电子商务的一种网络安全协议。SSL 刚开始制定时是面向 Web 应用的安全解决方案，目前 SSL 已经成为 Web 上最为广泛的信息安全协议之一，大部分 Web 服务器和浏览器都内置了该协议，比较容易应用。

1. SSL 概述

在 Internet 体系结构中，套接字层(Socket Layer)位于应用层和传输层之间。而套接字(Socket)的概念起源于 20 世纪 80 年代的 UNIX 操作系统，它定义了客户机与服务器之间进行的通信方式。这种通信方式既可以是面向连接的(如使用 TCP 协议)，也可以是面向非连接的(如使用 UDP 协议)。Socket 可以看成是通信中的一个端点，其中客户机上的应用程序利用一个 Socket 地址来呼叫服务器上的 Socket，一旦服务器上的 Socket 与客户机上的 Socket 建立了连接，这两台计算机之间就可以交换数据。

SSL 是一种点对点之间构造的安全通道中传输数据的协议，它运行在传输层之上，应用层之下，是一种综合利用对称密钥和公开密钥技术进行安全通信的工业标准。在通信过程中，允许一个支持 SSL 协议的服务器在支持 SSL 协议的客户端使协议本身获得信任，使客户端得到服务器的信任，从而在两台机器间建立一个可靠的传输连接。SSL 协议主要提供了 3 个方面的安全服务。

(1) 认证。利用数字证书技术和可信任的第三方认证机构，为客户机和服务器之间的通信提供身份认证功能，以便于彼此之间进行身份识别。为了验证证书持有者的合法性，防止出现用户名欺骗，SSL 要求证书持有者在进行握手时相互交换数字证书，通过验证证书来保证对方的合法性。

(2) 机密性。在 SSL 客户机和服务器之间传输的所有数据都经过了加密处理，以防止非法用户进行窃取、篡改和冒充。

(3) 完整性。SSL 利用加密算法和 Hash 函数来保证客户机和服务器之间传输的数据的完整性。

如图 4-8 所示，SSL 协议分为上下两部分：上层为 SSL 握手协议，下层为 SSL 记录协议。其中 SSL 握手协议主要用来建立客户机与服务器之间的连接，并协商密钥；而 SSL 记录协议则定义了数据的传输格式。由此可以看出，SSL 协议是建立在可靠的传输层协议(如 TCP)之上的，与应用层协议无关，它在应用层协议通信之前就已经完成加密算法、通信密钥的协商以及服务器认证工作。高层的应用层协议(如 HTTP、FTP 和 Telnet 等)可以透明地建立在 SSL 协议之上，应用

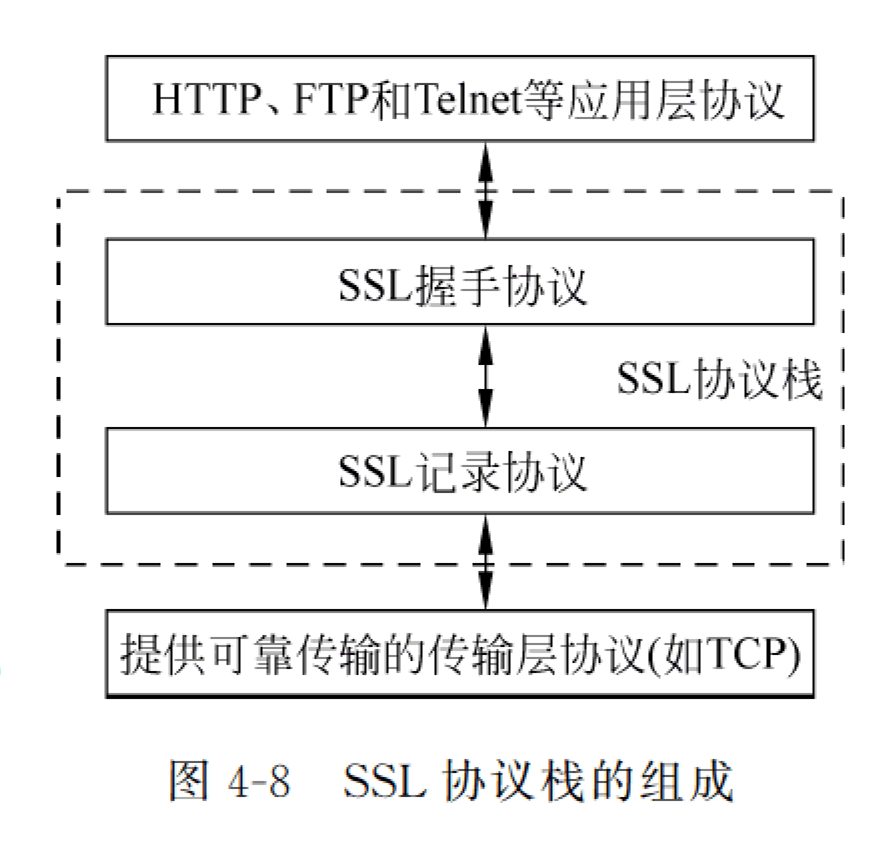


图 4-8　SSL 协议栈的组成

层协议所传送的数据都会被加密，从而保证通信的机密性。

2. SSL 握手协议

SSL 握手协议提供了客户机与服务器之间的相互认证，协商加密算法，用于保护在 SSL 记录中发送的加密密钥。握手协议在任何应用程序的数据传输之前进行。如图 4-9 所示，SSL 握手协议的一次握手操作包含以下几个过程。

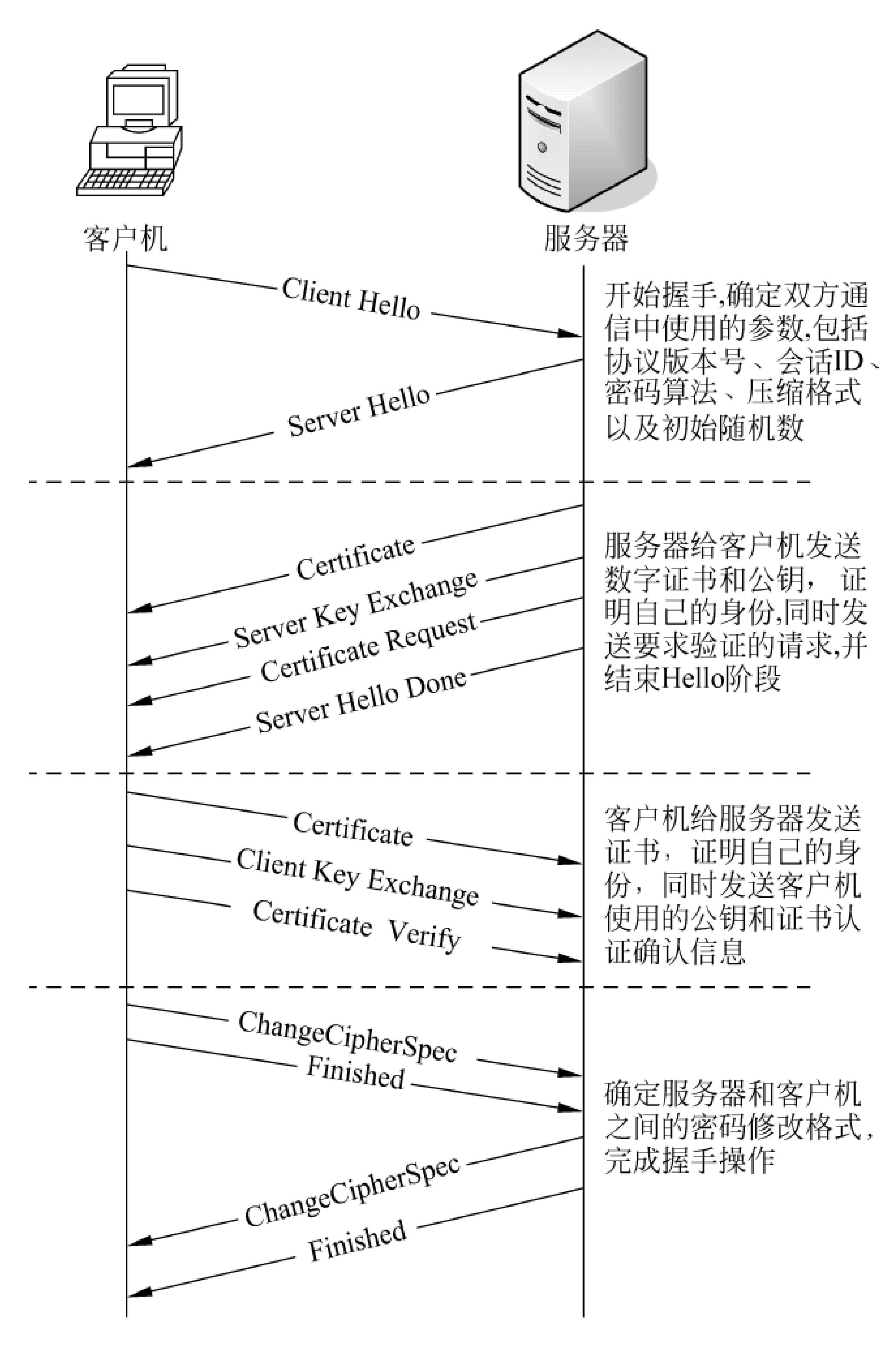


图 4-9　SSL 握手协议的操作过程

① 通信的初始化阶段。客户机向服务器发送一个会话消息(Client Hello)，服务器对该会话消息给予应答(Server Hello)。这一过程主要用于协商以下的信息：协议版本、加密算法、会话的 ID、压缩方法和一个初始随机数。其中，初始随机数是客户机与服务器之间对每个连接选择的字节序列。

② 如果客户机需要服务器的认证，则服务器开始发送它的数字认证证书，以证明其身份，包括证书消息(Certificate)、服务器密钥交换消息(Server Key Exchange)和证书请求消息(Certificate Request)。

③ 服务器发送一个服务器完成消息(Server Hello Done)，向客户机表明服务器的应答及提供的证书等消息已结束。

④ 客户机在接收到服务器的服务器完成消息后，如果收到了服务器发送的证书请求消息，即服务器需要对客户机进行认证，则客户机将向服务器发送证书消息。也可以不发送证书消息，客户机发送自己的密钥交换消息给服务器，发送之前需要用服务器公开密钥进行加密。如果服务器需要对客户机进行认证，同时客户机也接受了此请求，即客户机已经向服务器发送了证书消息，则客户机首先利用自己的私钥对已发送的证书消息进行数字签名，然后再发送给服务器，该签名后的消息为证书验证消息(Certificate Verify)，以证明自己是证书的真正持有者。

⑤ 客户机和服务器分别发送修改密码格式消息(ChangeCipherSpec)，完成密钥交换；客户端和服务器相互发送完成消息(Finished)，完成认证过程。

在 SSL 握手协议操作的任意步骤中，如果协商结果不符合某一方的要求，通信的任意一方都可以终止握手进程。在完成握手后，客户机和服务器即可以开始交换应用层数据。传输数据时，用对称密码进行加密，对称密钥用非对称算法加密，再把加密消息与被加密的密钥数据绑定后进行传输。接收的过程与发送过程正好相反，首先用接收者的私钥打开对称密钥的加密包，再用得到的对称密钥对消息进行解密，得到明文数据。

3. SSL 记录协议

SSL 记录协议建立在可靠的传输层协议(如 TCP)之上，为高层协议(如 HTTP、FTP 等)提供数据封装、压缩和加密等基本功能的支持。如图 4-10 所示，SSL 记录协议的操作过程如下。

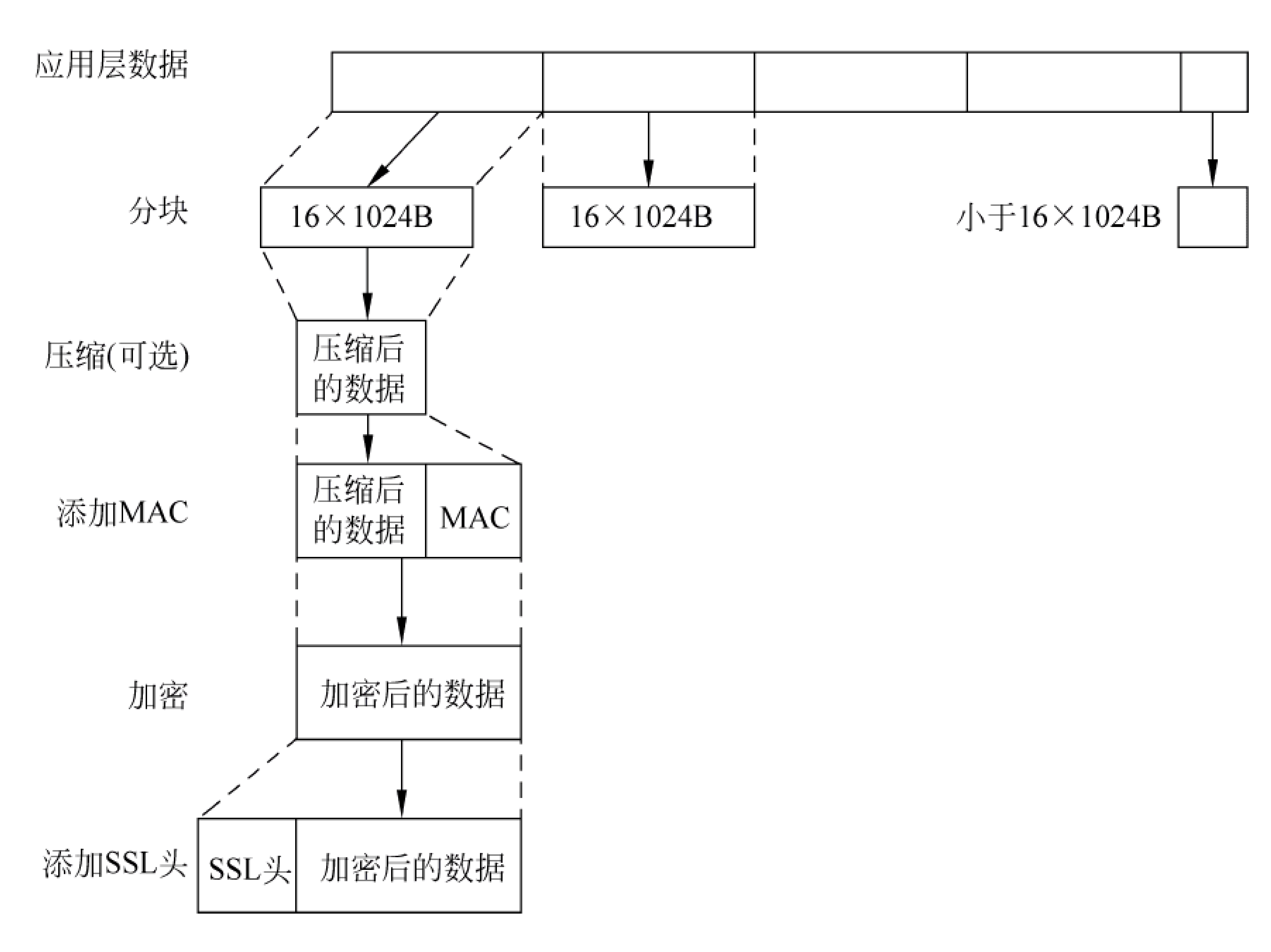


图 4-10　SSL 记录协议的操作过程

① 数据分块。将应用层的数据分解为大小为 16×1024B(其中 B 表示字节)或更小的数据块。

② 数据压缩(可选)。压缩必须是无损的，压缩后的数据长度未必比压缩前的数据短，但增加的内容长度不能超过 1024B。在 SSLv3 中，没有说明采用哪一种压缩方式，所以系

统默认为空，即不进行压缩。

③ 计算并添加 MAC（消息认证码）。对压缩后的数据，采用单向 Hash 函数计算 MAC，并添加到压缩后的数据后面。

④ 加密。对压缩数据和 MAC 进行加密。加密对数据长度的增加不能超过 1024B。允许采用的加密算法及相应的密钥长度如表 4-1 所示。

表 4-1　SSL 协议中使用的加密算法及其密钥长度

分组密钥		流密钥	
算法	密钥长度/位	算法	密钥长度/位
IDEA	128	RC4-40	40
RC2-40	40	RC4-128	128
DES-40	40		
3DES	168		
Fortezza	80		
DES	56		

⑤ 添加 SSL 记录头。在加密后的数据头部添加一个 SSL 记录协议头，使数据形成一个完整的 SSL 记录。该 SSL 记录头由以下字段组成（如图 4-11 所示）。

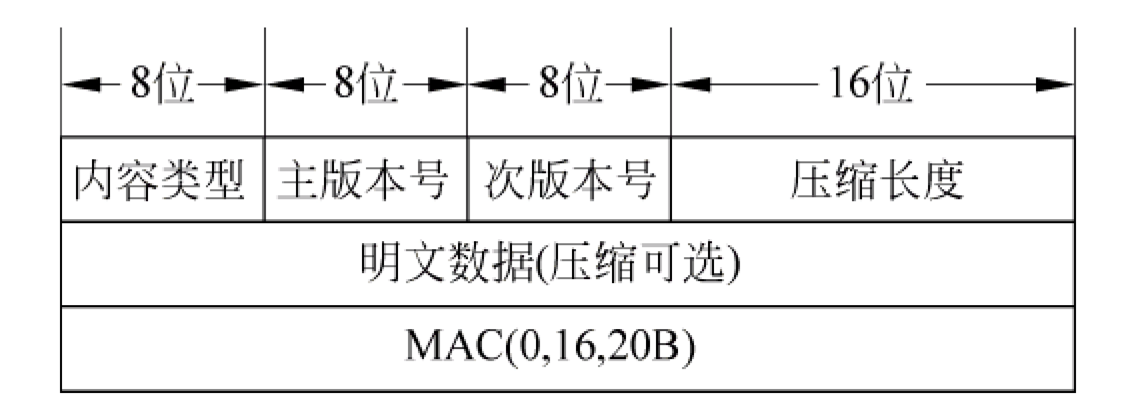


图 4-11　SSL 记录协议字段

（1）内容类型。封装的高层协议类型。

（2）主版本号。使用的 SSL 主版本号，如果采用 SSL v3 协议，该字段值为 3。

（3）次版本号。使用的 SSL 次版本号，如果采用 SSL v3 协议，该字段值为 0。

（4）压缩长度。以字节为单位的数据长度。有两种情况：如果采用了压缩，该字段值为压缩后的数据块长度；如果没有压缩，则该字段为明文数据块的长度。但两种长度都应该包括 MAC。

4. SSL 协议的特点

SSL 是一个通信协议。为了实现安全性，SSL 的协议描述比较复杂，具有较完备的握手过程。这也决定了 SSL 不是一个轻量级的网络协议。另外，SSL 还涉及到大量的计算密集型算法：非对称加密算法、对称加密算法和数据摘要算法。

IETF 将 SSL 进行了标准化，即 RFC 2246，并将其称为 TLS（Transport Layer Security）。从技术上讲，TLSv1.0 与 SSLv3.0 的差别非常小。有关 TLS 的详细介绍，读者可参阅相关的技术文档。

4.7 实验操作 1 基于 IEEE 802.1x 协议的 RADIUS 服务器的配置和应用

近年来，随着宽带网络应用的飞速发展，企业、学校、政府机关和居民小区等局域网纷纷通过身份认证方式接入 Internet。在这一过程中，如何实现对接入用户的认证、授权和审核（即 3A）是普遍关注的问题。基于 IEEE 802.1x 协议和 RADIUS 服务器的系统架构为这一问题提供了有效的解决方案。本实验立足目前的应用实际，介绍这些安全管理方式的实现过程。

4.7.1 实验设计

本实验是一个具有较大应用价值的综合实验。一是本实验立足目前的网络应用实际，可以直接在安全要求不太高的网络环境中使用；二是本实验的实现原理与目前市面上流行的计费认证系统基本相同，通过本实验可以帮助读者了解一些商业软件的功能特点；三是通过实践将会加深对本章前面介绍的理论知识的认识。

为便于实验的进行，设计了如图 4-12 所示的实验拓扑。其中，用于身份认证、授权和审计的 RADIUS 服务器由一台安装了“Internet 验证服务”组件的 Windows Server 2003 的计算机扮演，其 IP 地址为 172.16.2.10（读者也可以自定）。实验中使用的交换机必须是一台支持 IEEE 802.1x 协议的可网管交换机，在实验中需要启用交换机上的 IEEE 802.1x 协议。本实验使用了 Cisco3550 交换机，管理地址为 172.16.2.11。读者如果使用的是其他品牌或型号的交换机，只需要根据交换机的配置说明启用 IEEE 802.1x 协议即可，其他操作与本实验完全相同。由于 IEEE 802.1x 协议与 RADIUS 服务器之间良好的兼容性和互操作性，所以当客户端计算机通过 RADIUS 服务器认证访问网络资源（如接入 Internet）时，在客户端计算机上需要启用 IEEE 802.1x 协议。如果读者使用的计算机运行的是 Windows XP 及以上版本的操作，这些操作系统已内置了 IEEE 802.1x 协议，所以不需要单独安装客户端软件，否则还需要在客户端安装 IEEE 802.1x 认证软件。为了使本实验更贴近实际应用，还增加了一台应用服务器（IP 地址可以设置为 172.16.2.1），在该服务器上可以设置文件夹共享、FTP 或 Web 服务器，以便客户端测试使用。应用服务器在本实验中不是必需的。

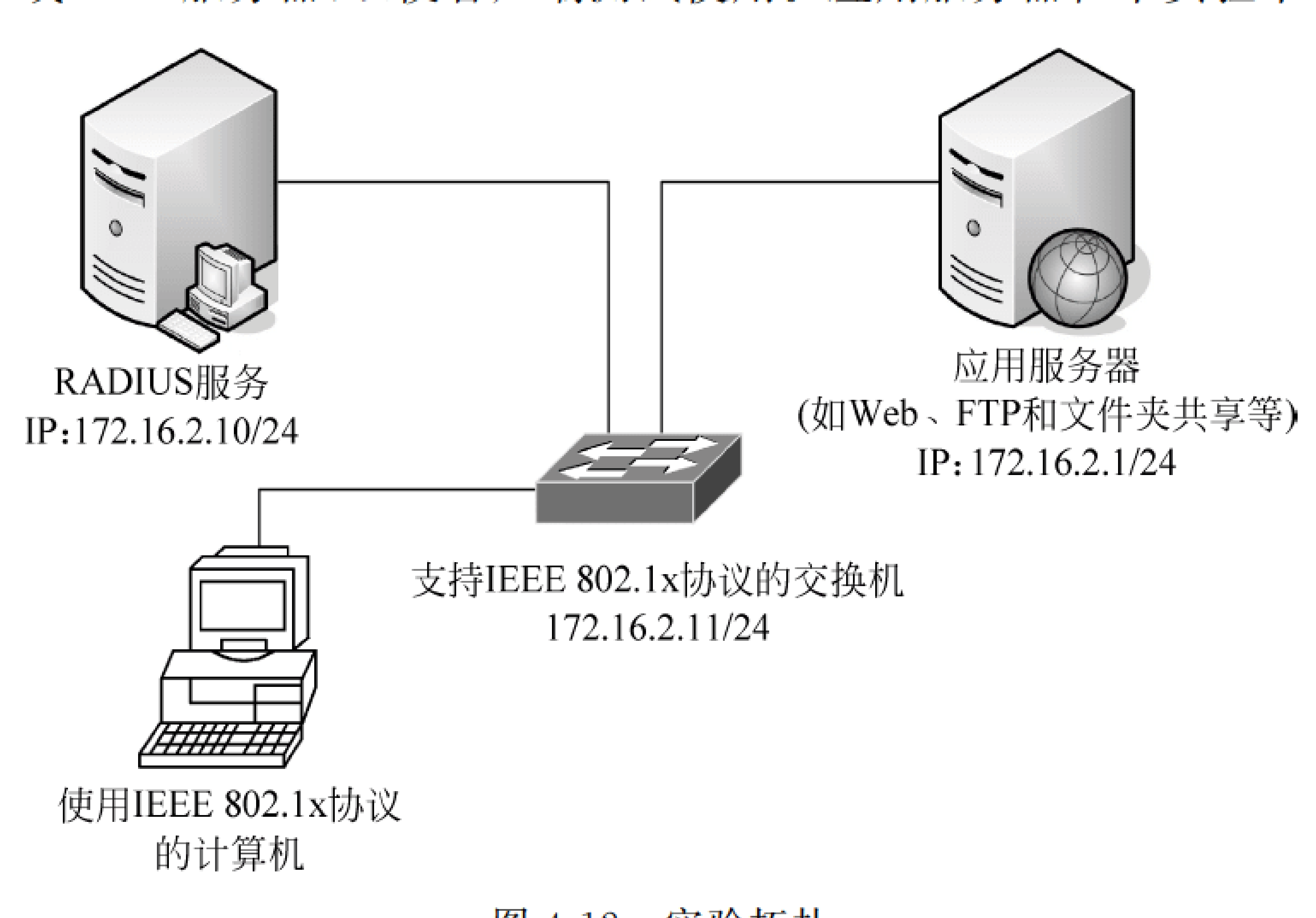


图 4-12 实验拓扑

4.7.2 IEEE 802.1x 和 RADIUS 服务器的概念

基于 IEEE 802.1x 和 RADIUS 服务器的身份认证系统目前已被用户广泛使用，为便于读者后面的操作，本小节首先介绍相关的概念。

1. IEEE 802.1x

IEEE 802.1x 是一个基于端口的网络访问控制协议，该协议的认证体系结构中采用了"可控端口"和"不可控端口"的逻辑功能，从而实现认证与业务的分离，保证了网络传输的效率。

IEEE 802 系列局域网标准占据着目前局域网应用的主要份额，但是传统的 IEEE 802 体系定义的局域网不提供接入认证，只要用户能接入集线器、交换机等控制设备，用户就可以访问局域网中其他设备上的资源。这是一个安全隐患，同时也不便于实现对局域网接入用户的管理。另外，在网吧等经营性场所中，设备提供者希望能对用户的接入进行认证、授权和计费。IEEE 802.1x 是一种基于端口的网络接入控制技术，在局域网设备的物理接入级对接入设备(主要是计算机)进行认证和控制。连接在交换机端口上的用户设备如果能通过认证，就可以访问局域网内的资源，也可以接入外部网络(如 Internet)；如果不能通过认证，则无法访问局域网内部的资源，同样也无法接入 Internet，相当于物理上断开了连接。

IEEE 802.1x 协议采用现有的可扩展认证协议(Extensible Authentication Protocol，EAP)，它是 IETF 提出的 PPP 协议的扩展，最早是为解决基于 IEEE 802.11 标准的无线局域网的认证而开发的。EAP 数据包含在 IEEE 802.1x 数据中，称为 EAPOL(EAP over LAN)，在证明者(Supplicant)和验证者(Authenticator)之间传输。验证者和验证服务器(Authentication Server)间同样运行 EAP 协议。EAP 帧中封装了认证数据，将该协议承载在 RADIUS 等其他高层协议中，以便穿越复杂的网络到达认证服务器，此过程称为 EAP over RADIUS。

虽然 IEEE802.1x 定义了基于端口的网络接入控制协议，但是在实际应用中该协议仅适用于接入设备与接入端口间的点到点的连接方式，其中端口可以是物理端口，也可以是逻辑端口。典型的应用方式有两种：一种是以太网交换机的一个物理端口，仅连接一台计算机；另一种是基于无线局域网的接入方式。其中，前者是基于物理端口的，而后者是基于逻辑端口的。目前，几乎所有的可网管以太网交换机都支持 IEEE 802.1x 协议。

2. RADIUS 服务器

RADIUS(Remote Authentication Dial In User Service，远程用户拨号认证服务)服务器提供了 3 种基本的功能：认证、授权和审计，即提供了 3A 功能。其中审计也称为"记账"或"计费"。

RADIUS 协议采用了客户机/服务器工作模式。网络接入服务器(Network Access Server，NAS)是 RADIUS 的客户端，它负责将用户的验证信息传递给指定的 RADIUS 服务器，然后处理返回的响应。RADIUS 服务器负责接收用户的连接请求，并验证用户身份，然后返回所有必须要配置的信息给客户端用户，也可以作为其他 RADIUS 服务器或其他类认证服务器的代理客户端。服务器和客户端之间传输的所有数据通过使用共享密钥来验证，客户端和 RADIUS 服务器之间的用户密码经过加密发送，提供了密码使用的安全性。

在如图 4-13 所示的网络中，RADIUS 服务器对 RADIUS 客户端(图 4-13 中直接标为

"客户端")进行用户验证、资源访问授权和记账等操作,主要操作过程如下。

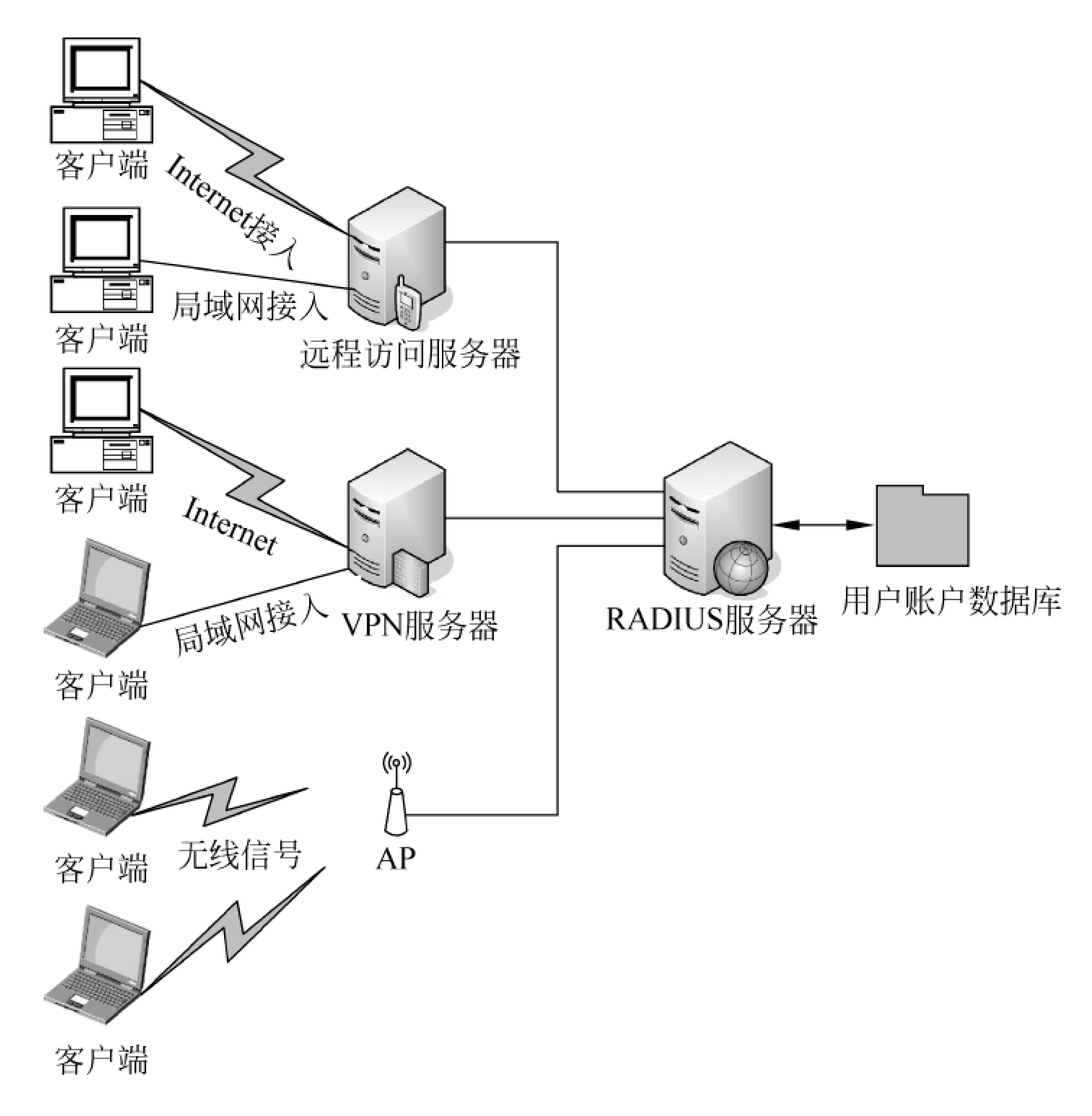


图 4-13　RADIUS 系统的组成

(1) 远程访问服务器、VPN 服务器和 AP 等接收到客户端的请求,然后将其直接转发给 RADIUS 服务器。

(2) RADIUS 服务器在用户账户数据库中检查该用户账户名称与密码的合法性,并根据已设置的访问策略来决定用户是否有权限来连接。此过程即进行用户身份验证、授权。

(3) 如果用户有权限来连接,RADIUS 服务器便会通知运行有用户账户数据库的服务器(该服务器称为"访问服务器"),再由"访问服务器"实现与客户端的连接。同时,"访问服务器"通知 RADIUS 服务器将此次连接进行记录,并启用记账功能(如果设置有记账功能的话)。

4.7.3　安装 RADIUS 服务器

下面在一台运行 Windows Server 2003 操作系统的计算机上通过安装"Internet 验证服务"组件,将其配置为一台 RADIUS 服务器。如果这台计算机是一台 Windows Server 2003 的独立服务器(未升级成为域控制器,也未加入域),则可以利用 SAM 来管理用户账户信息;如果是一台 Windows Server 2003 域控制器,则利用活动目录数据库来管理用户账户信息。虽然活动目录数据库管理用户账户信息要比利用 SAM 安全、稳定,但 RADIUS 服务器提供的认证功能相同。为便于实验,下面以一台运行 Windows Server 2003 的独立服务器为例进行介绍,该计算机的 IP 地址为 172.16.2.10。

另外,Linux 也提供了组件 RADIUS 服务器的功能,而且基于 Linux 的 RADIUS 服务器的运行要比 Windows 系统稳定。熟悉 Linux 的读者也可以组建基于 Linux 的 RADIUS

服务器完成此实验。

打开 Windows Server 2003 服务器，通过以下操作来安装 IAS 服务器。

(1) 选择"开始"→"设置"→"控制面板"→"添加或删除程序"→"添加/删除 Windows 组件"，在打开的如图 4-14 所示的"Windows 组件向导"对话框中选取"网络服务"组件。

(2) 单击"详细信息"按钮，在打开的如图 4-15 所示的"网络服务"对话框中选取"Internet 验证服务"子组件。

(3) 单击"确定"按钮，返回如图 4-14 所示的对话框。

(4) 单击"下一步"按钮，系统开始从 Windows Server 2003 安装光盘复制所需要的文件，直到最后安装结束。

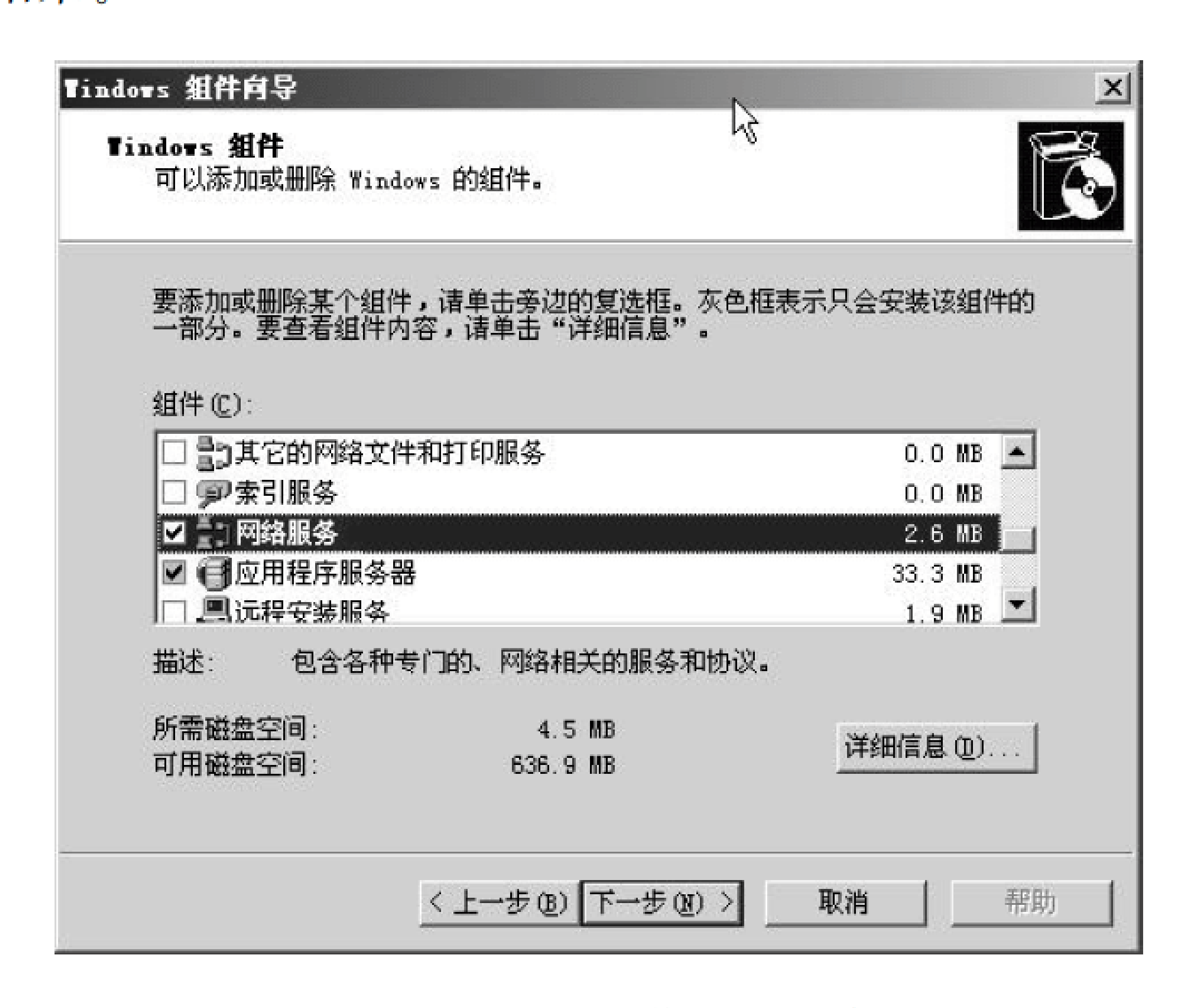


图 4-14　选择"网络服务"组件

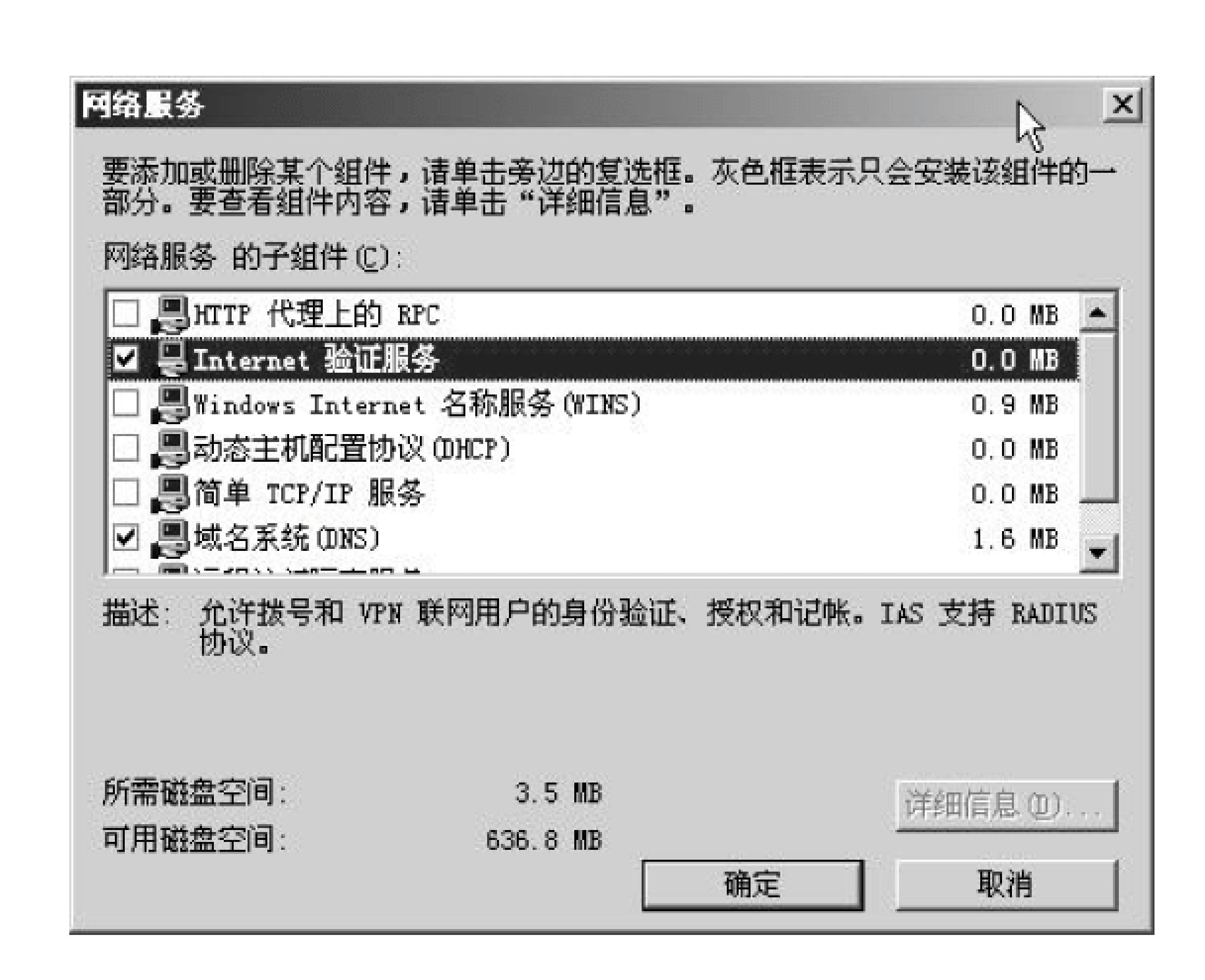


图 4-15　选取"Internet 验证服务"子组件

安装结束后，可以选择"开始"→"程序"→"管理工具"→"Internet 验证服务"打开如图 4-16 所示的"Internet 验证服务"窗口。在该窗口中，用户可以通过操作菜单或按钮来对相关服务进行操作，如停止服务、启用服务等。



图 4-16 “Internet 验证服务(本地)”窗口

如果用户要在自己的运行有 Windows Server 2003 的计算机上对 RADIUS 服务器进行远程管理，可以在本地计算机上选择“开始”→“运行”命令，在打开对话框的文本框中输入 MMC 命令。打开“控制台”窗口，在该窗口中选择“文件”→“添加/删除管理单元”→“添加”→“Internet 验证服务”→“添加”→“另一台计算机”，在打开的对话框中输入远程 RADIUS 服务器的 IP 地址，创建管理控制台，通过管理控制台对远程 RADIUS 服务器进行管理。

需要说明的是，如果读者是通过域控制器的 Active Directory 数据库来进行用户账户的管理，则需要建立 IAS 服务器与 Active Directory 数据库之间的连接。这样，当 RADIUS 客户端需要进行身份验证、授权或记账等操作时，就通过 Active Directory 数据库来完成。

4.7.4 创建 RADIUS 客户端

需要说明的是，这里要创建的 RADIUS 客户端，是指类似于图 4-12 中的交换机设备。在实际应用中也可以是 VPN 服务器、无线 AP 等，而不是用户端的计算机。

RADIUS 服务器只会接受由 RADIUS 客户端设备发过来的请求，为此需要在 RADIUS 服务器上来指定 RADIUS 客户端。以图 4-12 为例，具体步骤如下。

(1) 在 IAS 服务器上，打开“Internet 验证服务”窗口，然后选取“RADIUS 客户端”，单击鼠标右键，在弹出的快捷菜单中选择“新建 RADIUS 客户端”命令，如图 4-17 所示。

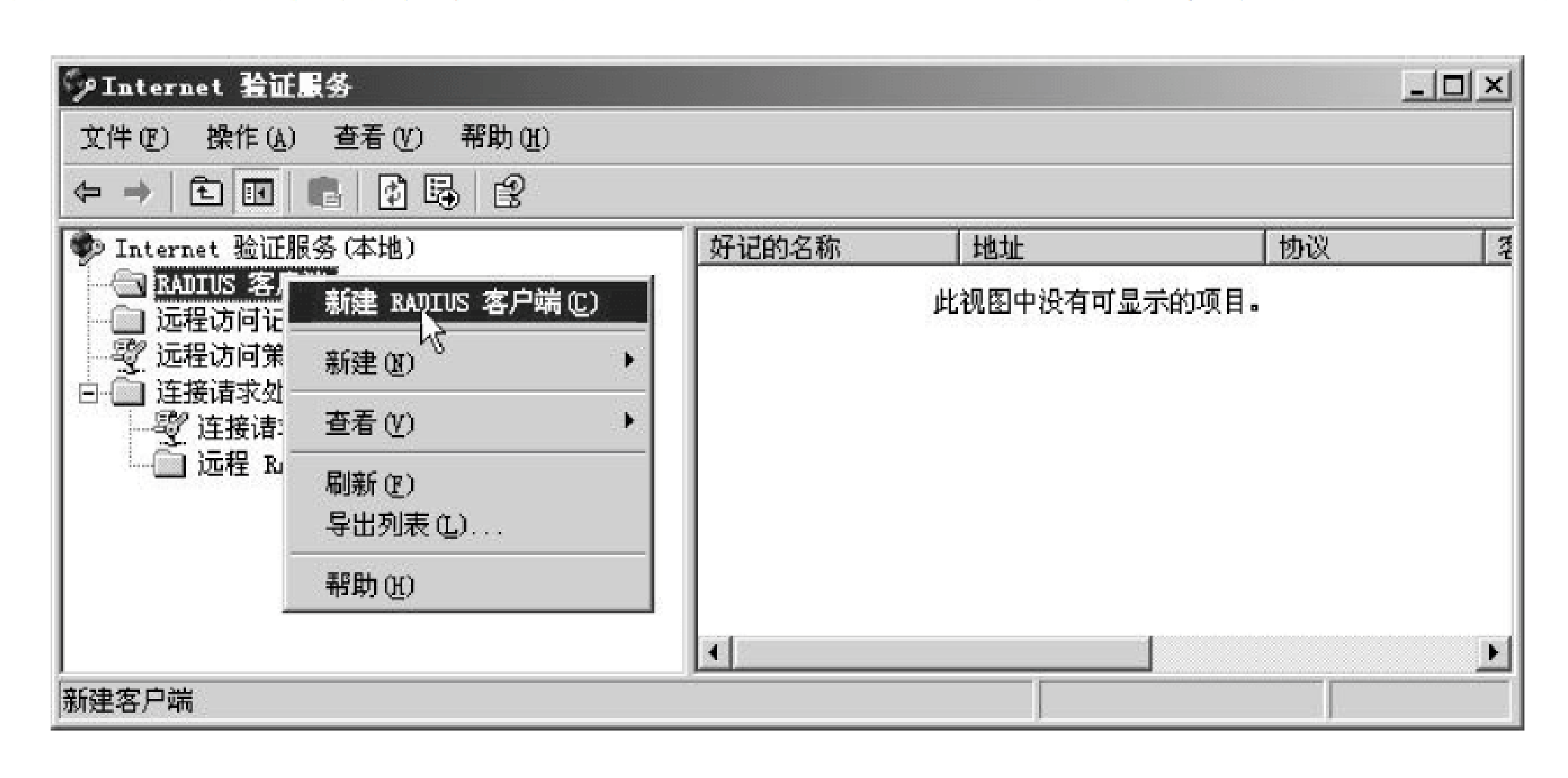


图 4-17 “新建 RADIUS 客户端”窗口

（2）在打开的如图 4-18 所示的“新建 RADIUS 客户端”对话框中，为此 RADIUS 客户端输入一个名称，并输入该客户端的 IP 地址或主机名称。为确认输入的 IP 地址或主机名称的正确性，可以单击“验证”按钮进行验证。



图 4-18　设置 RADIUS 客户端的名称和 IP 地址

（3）单击“下一步”按钮，在如图 4-19 所示的对话框中设置客户端的安全验证方式及共享密钥。



图 4-19　设置共享密钥和认证方式

① 客户端-供应商。用于选择提供 RADIUS 客户端软件的供应商，用户可根据 RADIUS 客户端的实际情况来选择，Windows Server 2003 的 RADIUS 服务器支持大量的 RADIUS 客户端软件。例如，当 RADIUS 客户端运行的是 Windows 操作系统时，可以选择 Microsoft。如果在这里找不到用户所需要的 RADIUS 客户端软件，则选择 RADIUS Standard 即可。由于本例是结合 IEEE 802.1x 协议进行身份认证，所以选择 RADIUS Standard。

② 共享的机密。在这里可以为 RADIUS 客户端设置一个密钥，这样当该客户端用户

在登录时必须正确输入此密码，RADIUS 服务器才会进行身份验证、授权和记账等操作。注意，输入密码时需要注意大小写。

③ 请求必须包括消息验证程序属性。如果双方所采用的验证方式是 PAP、CHAP、MS-CHAP 和 MS-CHAP v2，则 RADIUS 服务器端可以让客户端发送“消息验证程序属性”，以提高数据传输的安全性。如果验证方式采用 EAP，则 RADIUS 客户端会自动启用此功能，不需要单独进行设置。

④ 单击“确定”按钮，一个 RADIUS 客户端创建完成，如图 4-20 所示。



图 4-20 显示已创建的 RADIUS 客户端

如果网络中还有其他需要进行认证的设备，读者可以采取相同的方法来创建其他的 RADIUS 客户端。

4.7.5 创建用户账户

在这一节中，需要为所有通过认证才能够访问网络的用户在 RADIUS 服务器中创建账户。这样，当用户的计算机连接到启用了端口认证功能的交换机上的端口上时，启用了 IEEE 802.1x 认证功能的客户端计算机需要用户输入正确的账户和密码后，才能够访问网络中的资源。下面创建一个测试用的用户账户（如 wq），并设置相应的密码。具体方法为：选择“开始”→“程序”→“管理工具”→“计算机管理”→“系统工具”→“本地用户和组”→“用户”，单击鼠标右键，在弹出的快捷菜单中选择“新用户”命令，在打开的如图 4-21 所示的“新用户”对话框中进行创建。

图 4-21 创建用户账户

为便于对用户进行集中管理，还需要创建一个组，将所有的用户账户添加到组中进行统一管理。具体方法为：选择“开始”→“程序”→“管理工具”→“计算机管理”→“系统工具”→“本地用户和组”→“组”命令，单击鼠标右键，在弹出的快捷菜单中选择“新建组”命令，在出现的“新建组”对话框中输入组名(如 802.1x)，然后单击“添加”按钮，将前面新创建的用户添加到组中，如图 4-22 所示。单击“创建”按钮进行确认。



图 4-22　创建组并添加用户账户

另外，选择“开始”→“运行”命令，在打开的对话框中输入组策略编辑器命令 gpedit.msc，单击“确定”按钮，在出现的“本地安全设置”窗口中依次选择“计算机配置”→“Windows 设置”→“安全设置”→“账户策略”→“密码策略”，启用“用可还原的加密来储存密码”策略项，如图 4-23 所示。

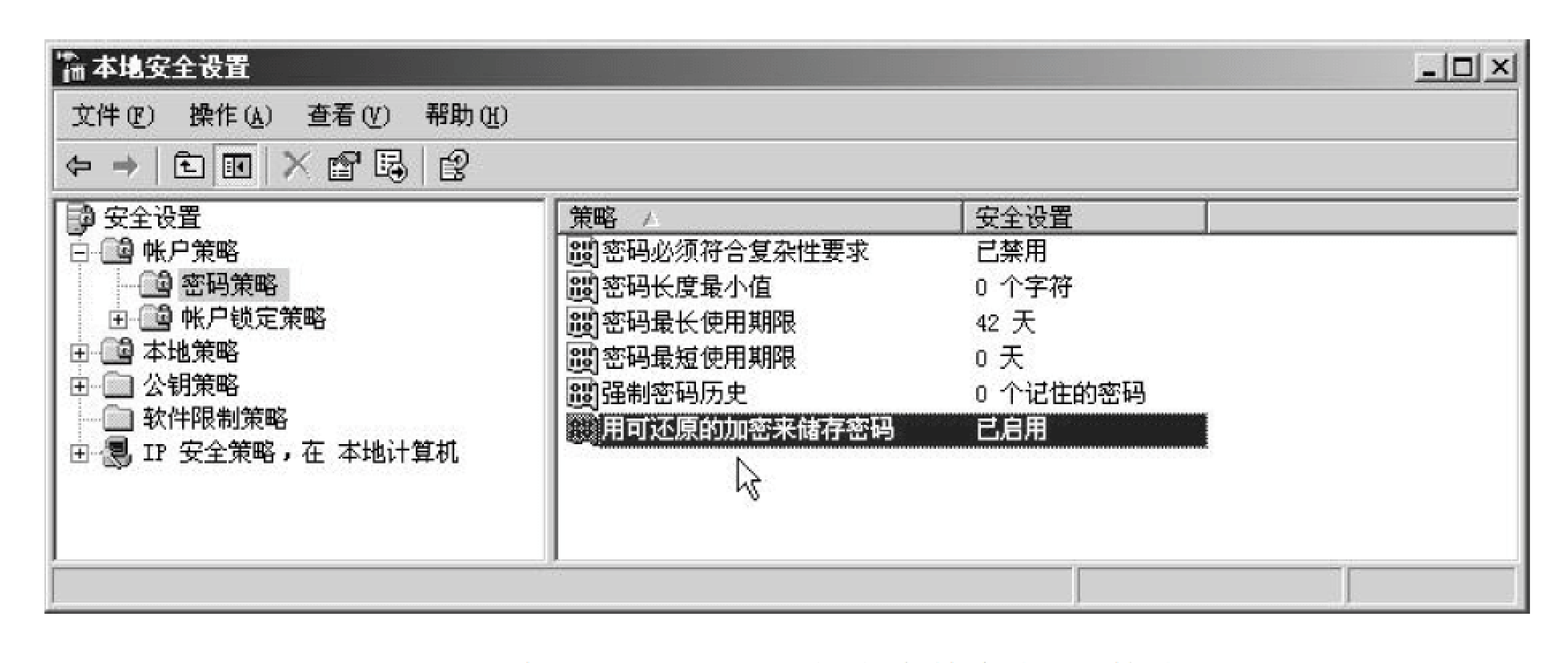


图 4-23　启用“用可还原的加密来储存密码”策略项

4.7.6　设置远程访问策略

下面在 RADIUS 服务器的“Internet 验证服务”窗口中，需要为图 4-12 中的交换机及通过该交换机进行认证的用户设置远程访问策略。具体方法如下。

(1) 在“Internet 验证服务”窗口中选取“远程访问策略”，单击鼠标右键，在弹出的快捷菜单中选择“新建远程访问策略”命令，如图 4-24 所示。



图 4-24　新建远程访问策略

(2) 在随后出现的“新建远程访问策略向导”对话框中直接单击“下一步”按钮，打开如图 4-25 所示的对话框。选择“使用向导来设置普通情况下的典型的策略”单选按钮，并输入一个“策略名”。

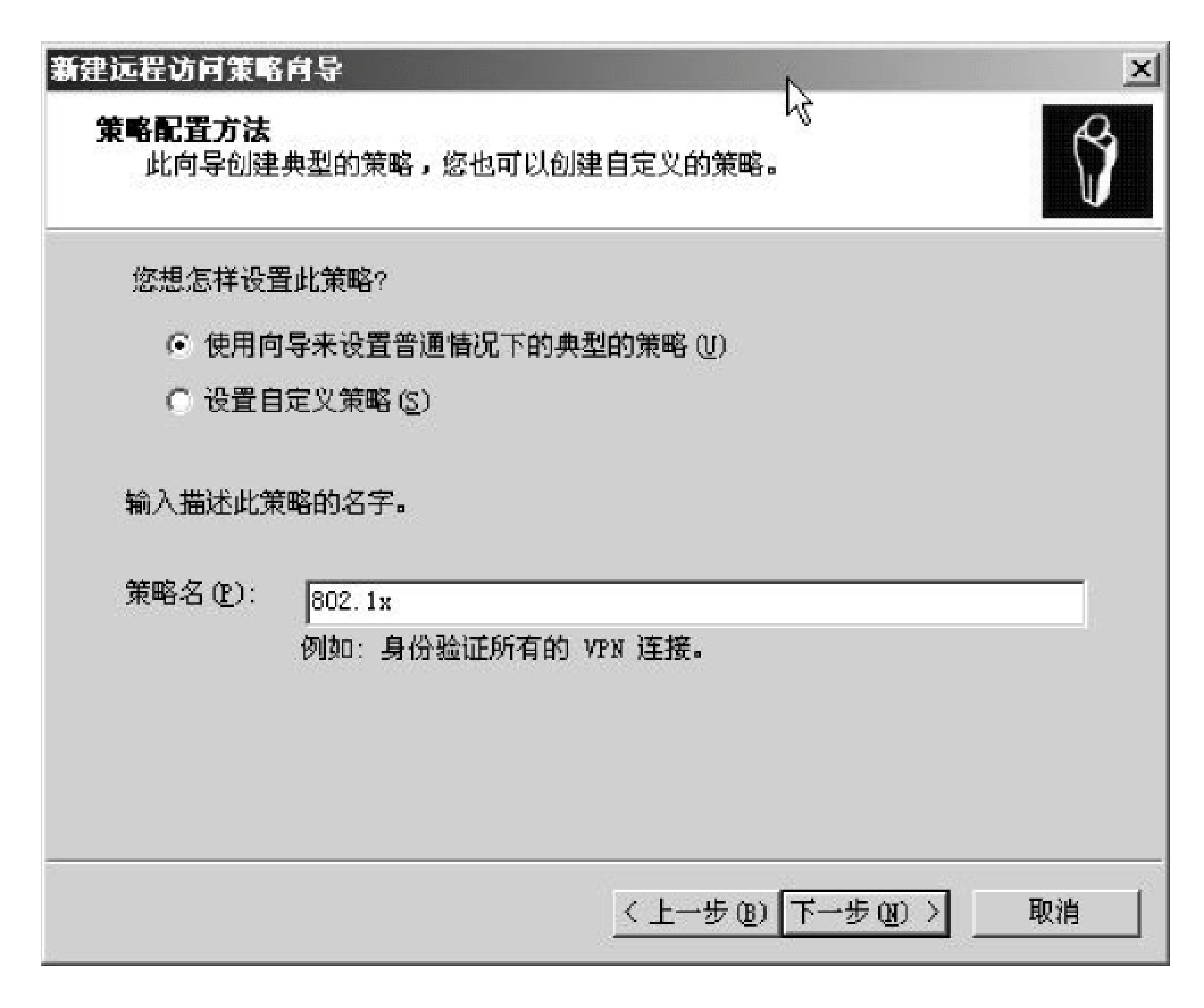


图 4-25　选择配置方式

(3) 单击“下一步”按钮，打开如图 4-26 所示的对话框。由于本实验是基于局域网而实现的，所以选择“以太网”单选按钮。

(4) 单击“下一步”按钮，在打开的如图 4-27 所示的对话框中选择是单独对“用户”进行授权，还是通过“组”来授权。由于已经为需要进行认证的用户创建了组(本例为 802.1x)，所以在这里选择“组”单选按钮，然后单击“添加”按钮，将前面创建的组名(802.1x)添加到“组名”列表框中。

(5) 单击“下一步”按钮，打开如图 4-28 所示的对话框。在“类型”下拉列表中选择身份验证类型，本实验选择 IEEE 802.1x 支持的“MD5-质询”类型。

(6) 单击“下一步”按钮，出现如图 4-29 所示的对话框。确认已设置的信息无误后，单击“完成”按钮，返回“Internet 验证服务”窗口。

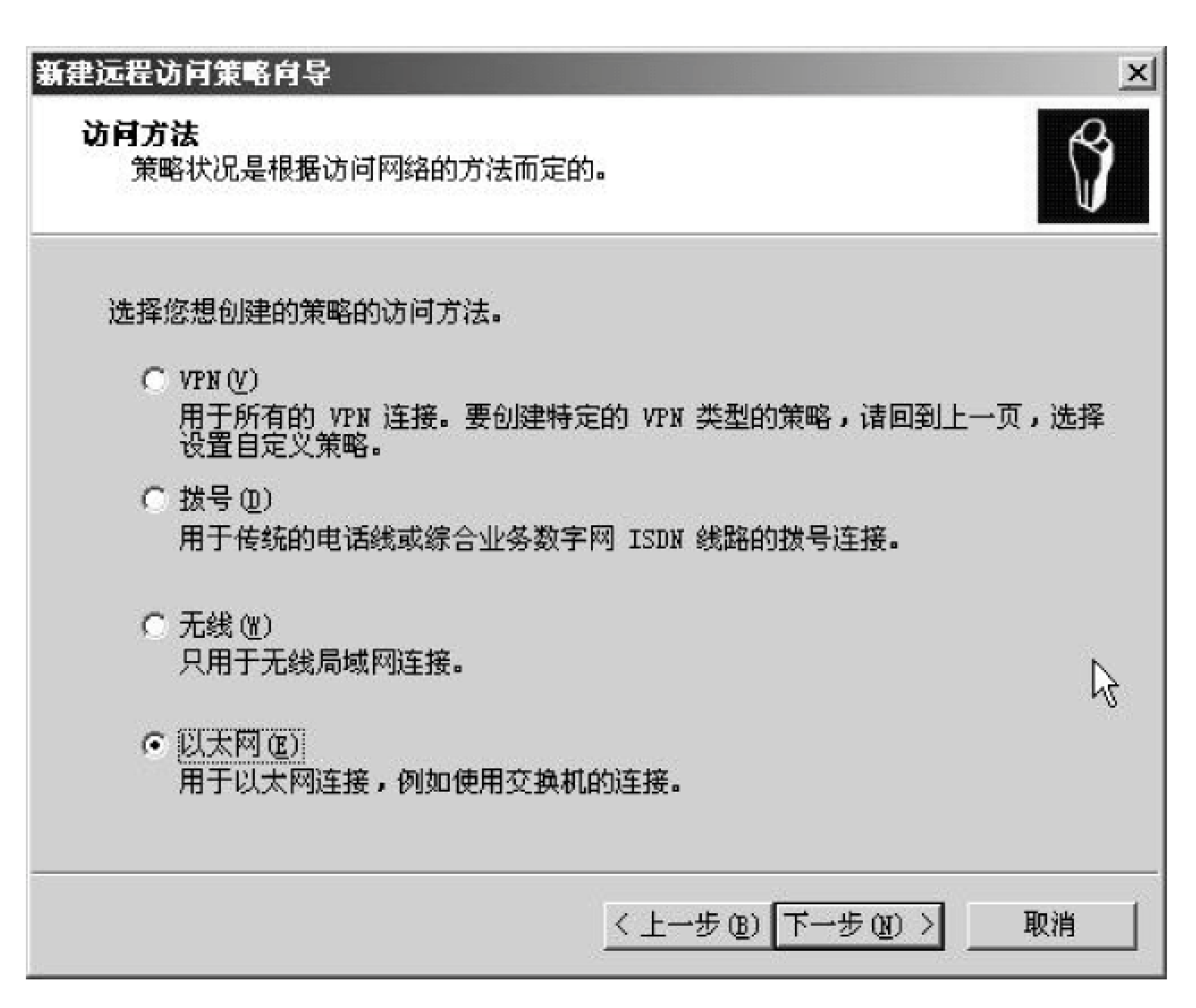


图 4-26　选择访问方法

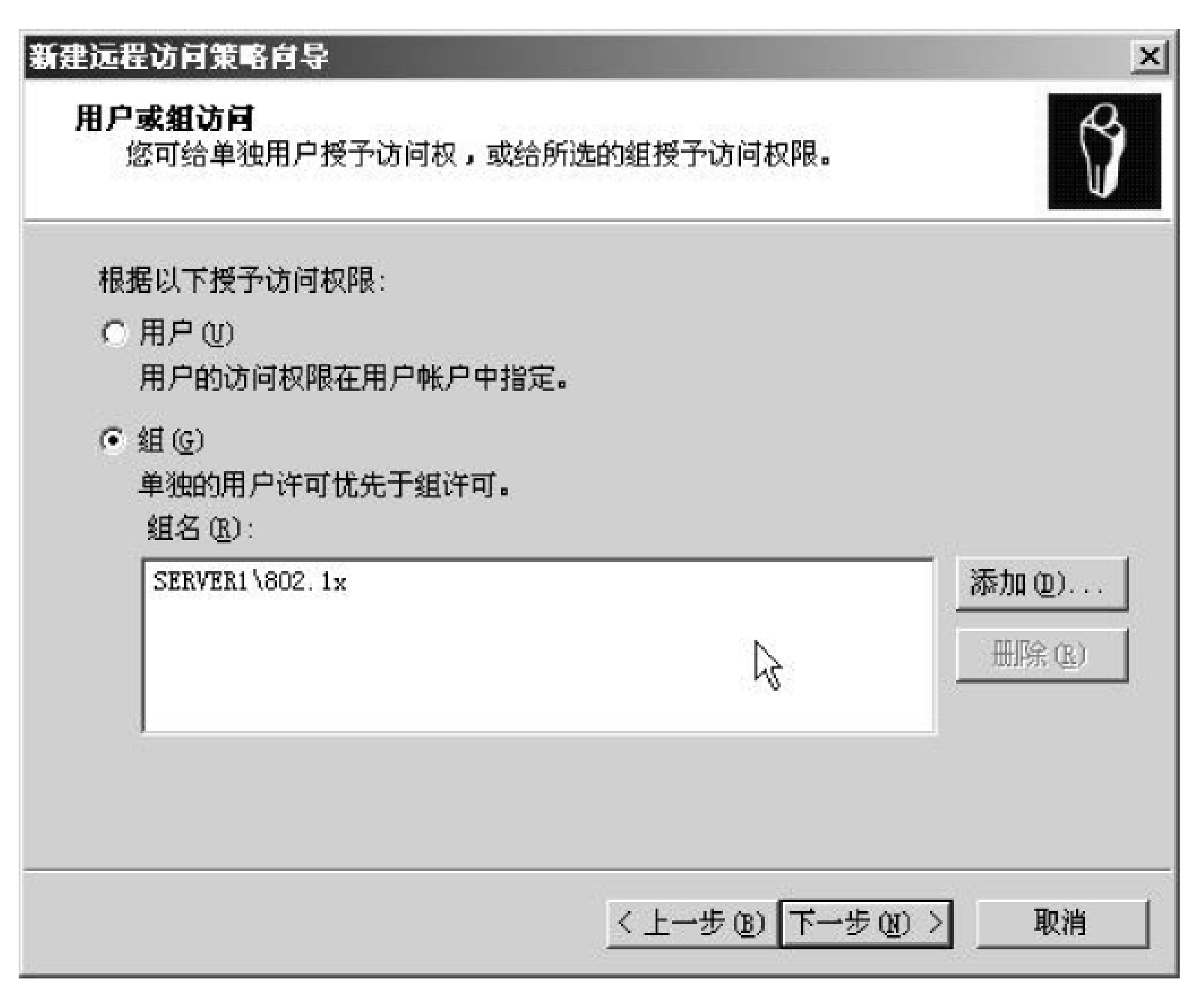


图 4-27　选择授权方式



图 4-28　选择身份验证方法

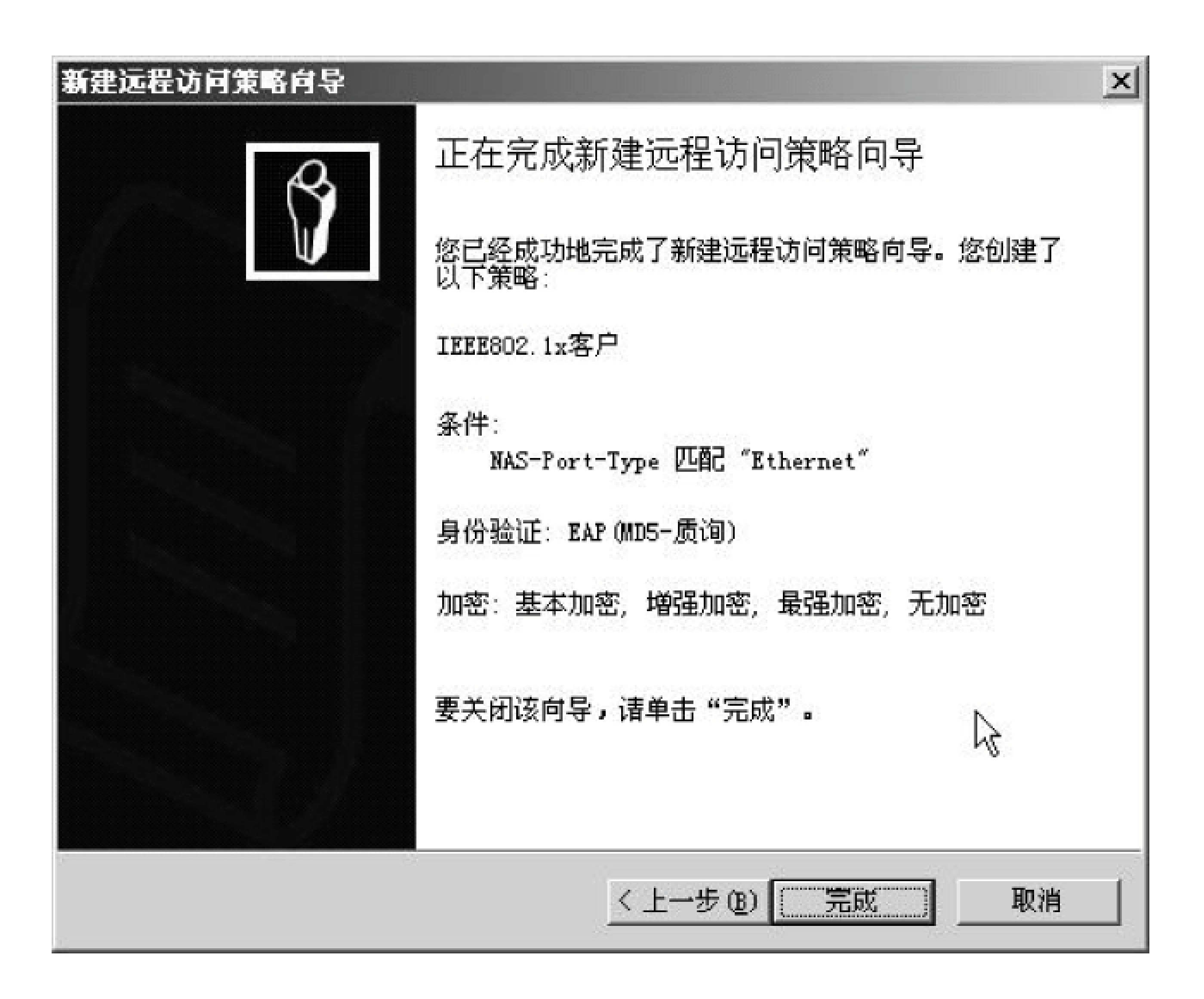


图 4-29　确认设置信息

（7）删除其他的远程访问策略，只保留新建的远程访问策略，最后如图 4-30 所示。

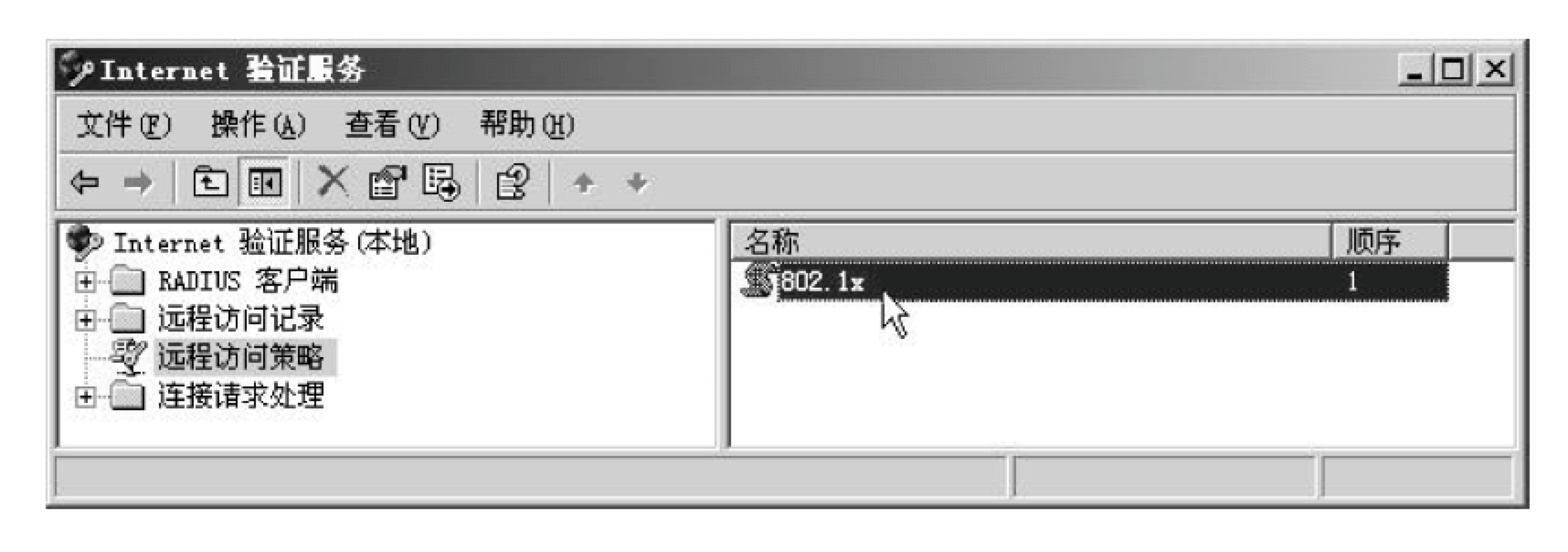


图 4-30　只保留新建的远程访问策略

（8）选取已创建的远程访问策略（本实验为 802.1x），单击鼠标右键，在弹出的快捷菜单中选择"属性"命令，并在打开的对话框中单击"添加"按钮，在出现的如图 4-31 所示的"选择属性"对话框中选择 Windows-Groups 选项，然后单击"添加"按钮。在出现的对话框中再单击"添加"按钮，将为需要进行认证的用户创建的组添加到"策略状况"列表中，如图 4-32 所示。



图 4-31　选择属性类型

（9）单击“确定”按钮，完成设置。



图 4-32　显示已添加的策略名称

4.7.7　交换机(RADIUS 客户端)的配置

下面对支持 IEEE 802.1x 认证协议的交换机进行配置，使它能够接受用户端的认证请求，并将请求转发给 RADIUS 服务器进行认证，最后将认证结果返回给用户端。其实，这里的交换机有些类似于代理的功能。

以图 4-12 为例，交换机的 IP 地址为 172.16.2.11/24，在交换机上只需要对 FastEthernet 0/1 端口进行认证，其他端口可不进行设置。所以，在本实验中，图 4-12 中的 RADIUS 服务器和应用服务器不要接在认证端口上。具体操作如下。

（1）设置交换机的管理地址。由于交换机在接收到用户的认证请求后，要将该请求发送给 RADIUS 服务器，然后还要将认证结果返回给用户。所以，必须给交换机配置一个管理地址，用该地址实现交换机与 RADIUS 服务器之间的通信。交换机的地址已在 4.7.4 节的图 4-18 中指定，本例为 172.16.2.11/24。在交换机上的配置如下。

Cisco3550#*conf t*　（进入交换机配置模式）

Cisco3550(config)#*interface vlan* 1　（选择虚拟接口 VLAN1，注意二层交换机的管理地址都配置在 interface vlan 1 上）

Cisco3550(config-if)#*ip address 172.16.2.11 255.255.255.0*　（设置管理地址为 172.16.2.11）

Cisco3550(config-if)#*end*　（退出配置模式）

Cisco3550#*wr*　（进行保存）

（2）启用 AAA 认证。具体配置如下。

Cisco3550(config)#*aaa new-model*　（启用 AAA 认证）

Cisco3550(config)#*aaa authentication dot1x default group radius*　（启用 dot1x 认证）

Cisco3550(config)#*dot1x system-auth-control* (启用全局 dot1x 认证)

Cisco3550(config-if)#*end* (退出配置模式)

Cisco3550#*wr* (进行保存)

以上的 dot1x 即启用 IEEE 802.1x 认证。

(3) 指定 RADIUS 服务器的 IP 地址及交换机与 RADIUS 服务器之间的共享密钥。

Cisco3550(config)# *radius-server host 172.16.2.10 auth-port* 1812 *acct-port 1813 key wangqun*

Cisco3550(config)#*radius-server retransmit 3* (与 RADIUS 服务器之间的尝试连接次数为 3 次)

Cisco3550(config-if)#*end* (退出配置模式)

Cisco3550#*wr* (进行保存)

在以上命令中,172.16.2.10 为 RADIUS 服务器的 IP 地址,1812 是 RADIUS 服务器默认的认证端口,1813 是系统默认的计账端口。其中,auth-port 1812 acct-port 1813 可以省略。Key 后面的 wangqun 为交换机与 RADIUS 服务器之间的共享密钥(在图 4-19 中设置)。

(4) 配置交换机的认证端口。下面将交换机的第一个端口 FastEthernet 0/1 设置为需要进行 IEEE 802.1x 认证的端口。具体操作如下。

Cisco3550(config)#interface FastEthernet 0/1 (进入 FastEthernet 0/1 端口)

Cisco3550(config-if)# switchport mode access (将端口设置为访问端口)

Cisco3550(config-if)#dot1x port-control auto (将端口 802.1x 认证模式控制设置为自动)

Cisco3550(config-if)#dot1x timeout quiet-period 30 (设置认证失败后的重试时间为 30s)

Cisco3550(config-if)#dot1x timeout reauth-period 30 (设置认证失败后,进行重新认证的时间间距为 30s)

Cisco3550(config-if)#dot1x reauthentication (启用 802.1x 认证)

Cisco3550(config-if)#spanning-tree portfast (启用生成树协议,并设置为 portfast 端口)

Cisco3550(config-if)#*end* (退出配置模式)

Cisco3550#*wr* (进行保存)

关于交换机上 AAA 及 IEEE 802.1x 的相关配置及命令说明,读者可参阅相关的技术文档。

4.7.8 用户端连接测试

本实验中客户端计算机以 Windows XP SP2 为例进行介绍,具体步骤如下。

(1) 配置客户端的 IP 地址,如 172.16.2.13。

(2) 打开用户端计算机网络的"本地连接属性"对话框,然后选择"验证"选项卡,在打开的如图 4-33 所示的对话框中选取"启用此网络的 IEEE 802.1x 验证"复选框,并在"EAP 类型"下拉列表中选取"MD5-质询"选项,其他选项可不选。



图 4-33　启用客户端 IEEE 802.1x 验证

如果在打开“本地连接属性”对话框时，没有“验证”选项卡，需要选择“开始”→“设置”→“控制面板”→“性能和维护”→“管理工具”→“服务”，在打开的“服务”窗口中启用 Wireless Zero Configuration 即可。

(3) 将用户端计算机接到交换机的 FastEthernet 0/1 端口上，这时读者会发现交换机上 FastEthernet 0/1 端口对应的指示灯呈棕黄色，说明端口处于阻断状态。同时，在客户端任务栏的右下角将会出现如图 4-34 所示的提示信息。

这时，如果输入 Ping 172.16.2.1 命令，系统显示连接超时，说明客户端与应用服务器(如图 4-12 所示)之间无法进行通信。

(4) 单击图 4-34 中的本地连接图标，出现如图 4-35 所示的输入用户名和密码的“本地连接”对话框，“登录域”在本实验中可以不输入。

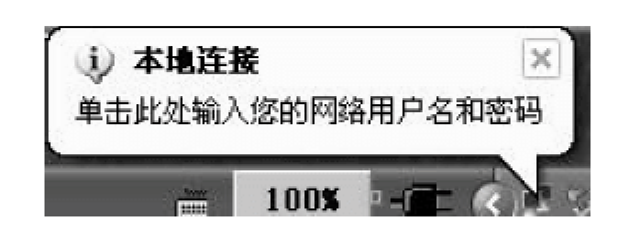


图 4-34　系统要求输入用户名和密码



图 4-35　输入用户名和密码的“本地连接”对话框

(5) 单击“确定”按钮，如果认证成功，交换机 FastEthernet 0/1 端口马上会呈现正常通信状态(显示为绿色)，同时在客户端 Ping 172.16.2.1，这时显示与应用服务器之间的连接

是正常的。

这时，在 RADIUS 服务器上打开“事件查看器”，在“系统”事件中将会显示用户的认证情况，如图 4-36 所示。为了进一步验证 RADIUS 服务器的认证，可以暂时断开与交换机 FastEthernet 0/1 端口的连接，当再次接入该端口，系统同样出现如图 4-34 所示的提示信息。当出现图 4-35 所示的对话框时，可以输入一个在 RADIUS 服务器上没有创建的用户账户（如 wangqun），单击“确定”按钮后，用户端提示“身份验证失败”，同时在 RADIUS 服务器的“系统”事件中，将会显示如图 4-37 所示的事件说明，对用户 wangqun 的认证未通过。



图 4-36　通过认证的用户事件记录

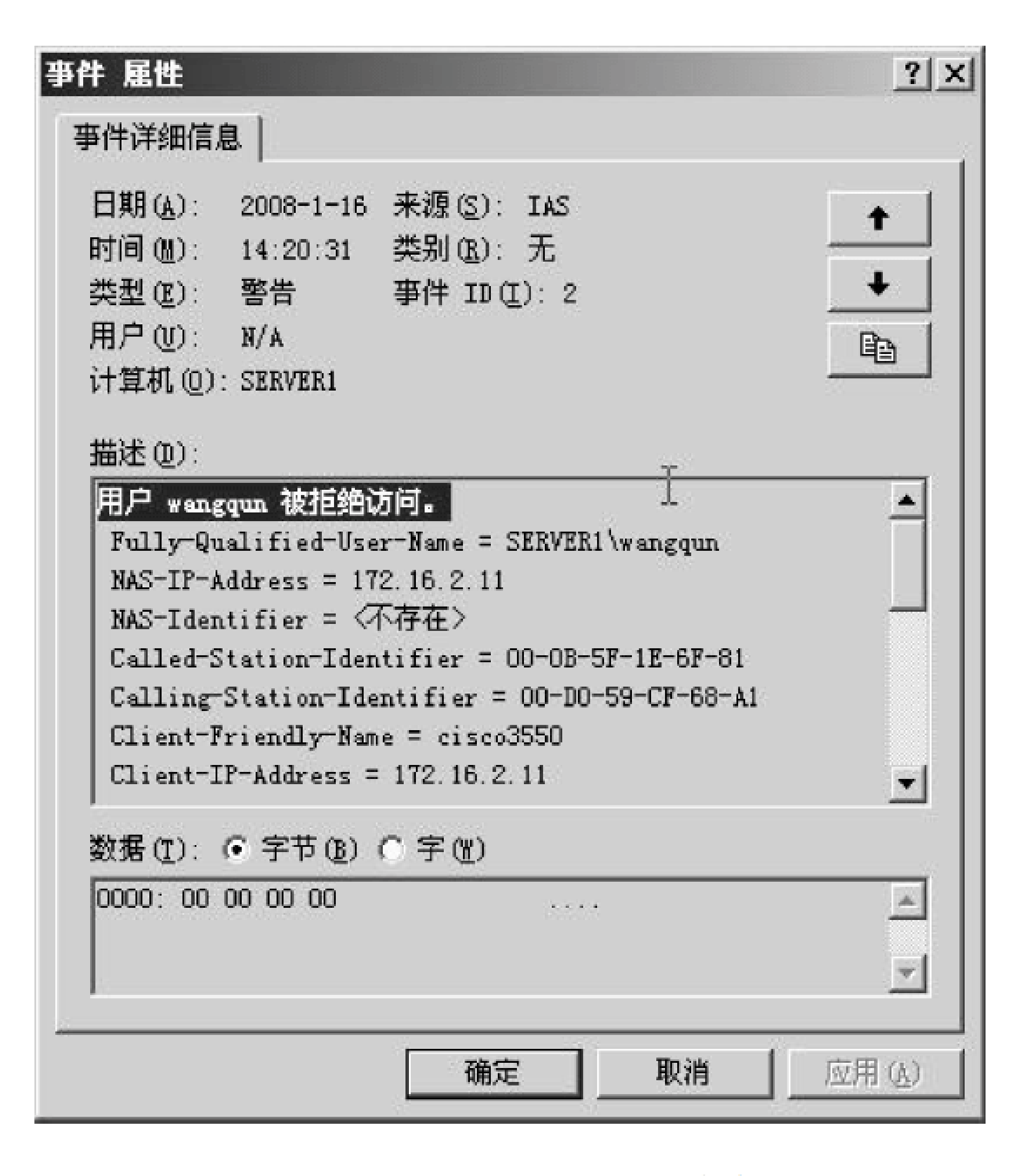


图 4-37　未通过认证的用户事件记录

本实验综合应用了身份认证的许多知识和技术细节，同时还可以与 CA 建立联系，由 CA 为用户发送证书，实现身份认证。这些内容读者可以查阅相关的技术文档，并通过实验加以掌握。另外，本实验具有较强的应用价值，希望读者联系网络应用实际，掌握实验的相关技术。

习　题

4-1　什么是身份认证？分析身份认证中 3 种不同方式的特点。

4-2　名称解释：认证、授权、审计。

4-3　在密码认证中如何设置和使用安全性高的密码？

4-4　介绍 Lamport 算法的过程和方法，说明一次性密码在密码认证中的特点。

4-5　名称解释：社会工程学、按键记录软件、搭线窃听、暴力破解、字典攻击、窥探、垃圾搜索、双因素认证。

4-6　什么是生物特征认证？与传统的密码认证等方式相比，生物特征认证有哪些优势？

4-7　什么是零知识证明认证？有什么特点？

4-8　简述 Kerberos 协议的特点及基本认证过程。

4-9　在 TCP/IP 体系结构中，SSL 协议是如何工作的？

4-10　简述 SSL 握手协议和 SSL 记录协议的工作过程。

4-11　简述 IEEE 802.1x 协议和 RADIUS 服务器的功能及应用特点。

4-12　参考如图 4-12 所示的网络拓扑，在实验室中独立完成该实验。

第5章 TCP/IP体系的协议安全

随着以Internet为主的互联网络的广泛应用，TCP/IP体系成为目前计算机网络的基础，IP网络已基本成为现代计算机网络的代名词。然而，由于当初设计TCP/IP体系时存在的局限性，以及随后信息技术对IP网络的依赖性，致使现在IP网络存在的安全问题日渐突出，各类安全隐患日显严重。本章以IPv4为基础，首先简要介绍TCP/IP体系的分层结构及各层的功能定义，然后联系实际应用，重点介绍TCP/IP协议栈中ARP、DHCP、TCP和DNS等子协议的安全问题及目前行之有效的安全防范方法。

5.1 TCP/IP体系

OSI参考模型的研究初衷是希望为网络体系与协议发展提供一种国际标准。但是，Internet在全球范围的飞速发展将TCP/IP体系推向了研究和应用的前台。在TCP/IP协议栈中已集成了大量的子协议并以Internet标准发布，同时随着Internet应用的不断发展，新的子协议及对已有协议的升级版本也将不断出现，并成为TCP/IP协议栈的成员。本节将简要介绍TCP/IP体系的分层特点及各层次的功能划分。

5.1.1 TCP/IP体系的分层特点

ARPAnet是应用最早的计算机网络类型之一，现代计算机网络的许多概念源自于ARPAnet。ARPAnet是由美国国防部资助的一个研究性网络，当初它通过租用的电话线将几百所大学和政府部门的计算机设备连接起来，要求通过一种灵活的网络体系结构实现不同设备、不同网络的互联和互通。后来卫星通信系统和无线电通信系统得到发展并应用到ARPAnet中，这时，ARPAnet最初开发的网络协议使用在通信可靠性较差的通信子网中时出现了问题，这就导致了TCP/IP协议的出现。

TCP/IP开始仅仅是两个协议：TCP（Transfer Control Protocol，传输控制协议）和IP（Internet Protocol，网际协议）。后来，TCP/IP演变为一种体系结构，即TCP/IP参考模型。现在的TCP/IP已成为一个工业标准的协议集，它最早应用于ARPAnet。因为当时的ARPAnet要求在任何条件下甚至是战争中都可以正常运行，这就决定了运行TCP/IP的网络具有很好的兼容性，并可以使用铜缆、光纤、微波及通信卫星等多种链路。同时，在TCP/IP网络中所有的数据都以分组的形式传输。

与OSI参考模型不同，TCP/IP模型由应用层（Application Layer）、传输层（Transport Layer）、网际层（Internet Layer，也称为Internet层）和网络接口层（Network Interface Layer）4部分组成，如图5-1所示。这4层大致对应OSI参考模型的7层。但与OSI模型不同的是，TCP/IP协议栈更加侧重于互连设备间的数据传送，而不是严格的功能层次的划分。

为了便于对 TCP/IP 体系的理解，可以将 TCP/IP 体系分为协议层和网络层两层，如图 5-2 所示。其中，协议层包括 TCP/IP 体系的上面两层（应用层和传输层），具体定义了有关网络通信协议的类型；而网络层包括 TCP/IP 模型的下面两层（网际层和网络接口层），具体定义了网络的类型（如局域网和广域网）和设备之间的路径选择。

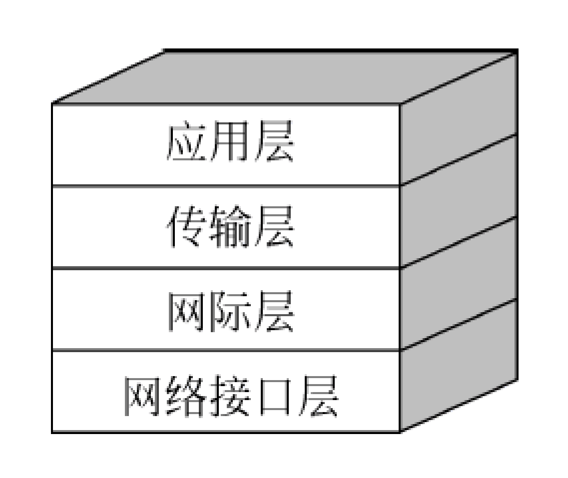


图 5-1　TCP/IP 体系

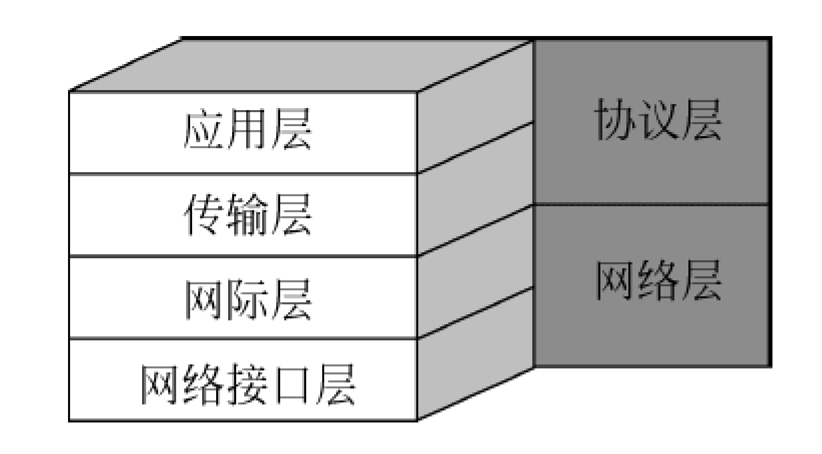


图 5-2　将 TCP/IP 体系划分为协议层和网络层

TCP/IP 是一个协议簇或协议栈，它是由多个子协议组成的集合。图 5-3 列出了 TCP/IP 体系中包括的一些主要协议及与 TCP/IP 体系的对应关系。理解这个图的结构（尤其是每一层对应的协议）对于后面的学习非常重要。

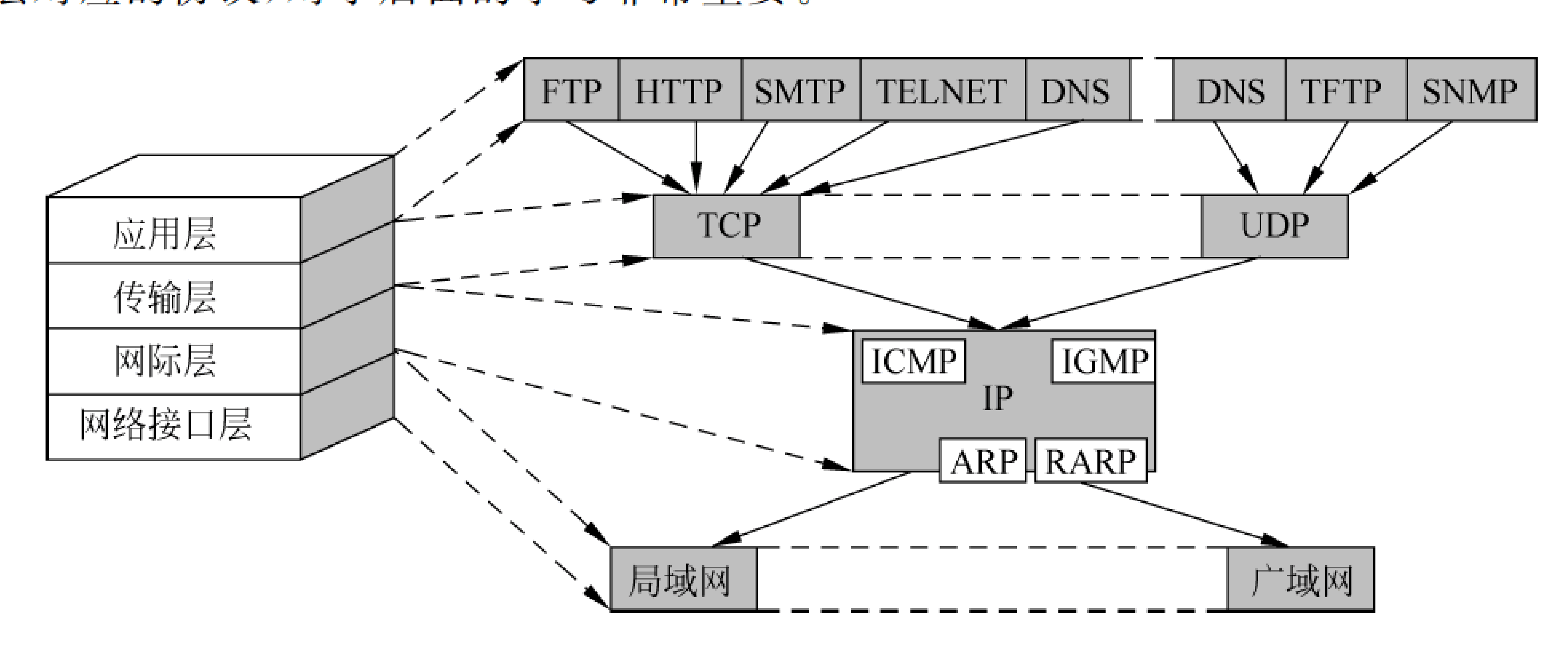


图 5-3　TCP/IP 体系中的主要协议及与各层的对应关系

5.1.2　TCP/IP 各层的主要功能

TCP/IP 体系也称为 TCP/IP 参考模型，该模型从下到上共分为网络接口层、网际层、传输层和应用层 4 个子层。各层的主要功能如下。

1. 网络接口层

在 TCP/IP 参考模型中，网络接口层属于最低的一层，它负责通过网络发送和接收分组。由于 TCP/IP 参考模型并没有明确规定在网络接口层应该使用哪些设备、网络和协议，这就带来了以下的好处：一是对于网际层及以上各层来说网络接口层是透明的，网际层及以上各层在功能实现过程中不需要考虑网络接口层使用的是什么类型的网络、设备或协议。二是有利于 TCP/IP 网络的发展。由于在 TCP/IP 参考模型中，网络接口层的定义是空白的，所以已有的各种类型的物理网络都可以作为 TCP/IP 的网络接口层存在，如目前已经使用的电路交换机、分组交换网（如 X.25、帧中继等）和局域网（如以太网、令牌网和 FDDI 等）。

2. 网际层

网际层也称为“互联网络层”，它相当于 OSI 参考模型网络层的无连接网络服务。网际层的任务是：允许位于同一网络或不同网络中的两台主机之间以分组的形式进行通信。更

具体地讲，网际层提供了以下的服务功能：一是处理从传输层接收下来的报文段发送请求，然后将报文段封装到 IP 数据报中，并根据源主机和目的主机的 IP 地址来填充报头，然后根据目的主机的 IP 地址选择一条链路将封装后的 IP 数据报发送出去。二是处理从网络接口层接收到的由其他主机发送过来的数据报，根据数据报中的目的地址决定这个数据报是发送给本主机的还是要发送给其他主机的。如果是发送给本主机的，则在去掉报头信息后提交给传输层；如果是发送给其他主机的，则根据数据报的目的 IP 地址选择一条链路进行转发。三是当本主机连接两个不同的网络(称为"子网")时，对接收到的数据报进行路由选择和转发，并进行流量控制和阻塞管理。

TCP/IP 参考模型中网际层的协议是唯一的，即 IP 协议。IP 协议是一个面向非连接的、不可靠的数据报传输服务协议，所以网际层的 IP 协议提供了一种"尽力而为(best-effort)"的服务。IP 协议的协议数据单元(PDU)称为分组，所以将 TCP/IP 网络也称为分组交换网络。

3. 传输层

在 TCP/IP 参考模型中，传输层位于网际层与应用层之间，其设计目标是：允许在源和目的主机的对等体之间进行会话，负责会话对等体的应用进程之间的通信。TCP/IP 参考模型的传输层功能类似于 OSI 参考模型传输层的功能。

在 TCP/IP 参考模型的传输层中定义了两个端到端的传输协议：传输控制协议 TCP 和用户数据报协议(User Datagram Protocol，UDP)。

其中，TCP 协议是一个可靠的、面向连接的协议，它实现了从一台主机发送出去的字节流(byte stream)无差错地传输到目的主机。在这一过程中，发送主机的传输层首先把从应用层接收到的数据流划分成为多个小的字节段(byte segment)，并对每一个字节段进行编号。然后，每一个字节段可以通过不同的路径到达目的主机，如果某一个字节段在传输过程中出错或丢失，则要求发送端进行重传。当目的主机接收到字节段后，根据其编号重组为原来的字节流，并提交给应用层进行处理。TCP 协议还负责处理流量控制，当发送端的发送速率与接收端的接收速度不匹配时(一般是发送速率大于接收速率)，调协收、发双方的速率，以确保字节段的可靠传输。

UDP 是一个不可靠的、面向非连接的传输层协议，主要用于不要求分组顺序到达的传输中，分组的先后顺序检查与排列由应用层的应用程序完成。同时，UDP 主要应用于"快速交付比精确交付更加重要"的应用，如语音传输、视频传输等。

4. 应用层

应用层属于 TCP/IP 参考模型的最高层。应用层主要包括根据应用需要开发的一些高层协议，如 TELNET、FTP、SMTP、DNS、SNMP 和 HTTP 等。而且，随着网络应用的不断发展，新的应用层协议还会不断出现。

需要说明的是，在 OSI 参考模型中，在传输层之上还定义了会话层和表示层，而在 TCP/IP 参考模型中却没有这两层。这是因为在当初设计时，研究人员认为 OSI 参考模型的高层划分过于复杂，而且每一层的功能设计并不明确或过于单一，这样在设计 TCP/IP 参考模型时就去掉了这两层。从目前的应用来看，TCP/IP 参考模型当初的这种设计是正确的。

5.1.3 TCP/IP 网络中分组的传输示例

在掌握了 TCP/IP 参考模型的分层特点及各层的功能后，下面通过一个具体的实例向读者介绍 TCP/IP 网络中分组的传输过程，网络拓扑如图 5-4 所示。

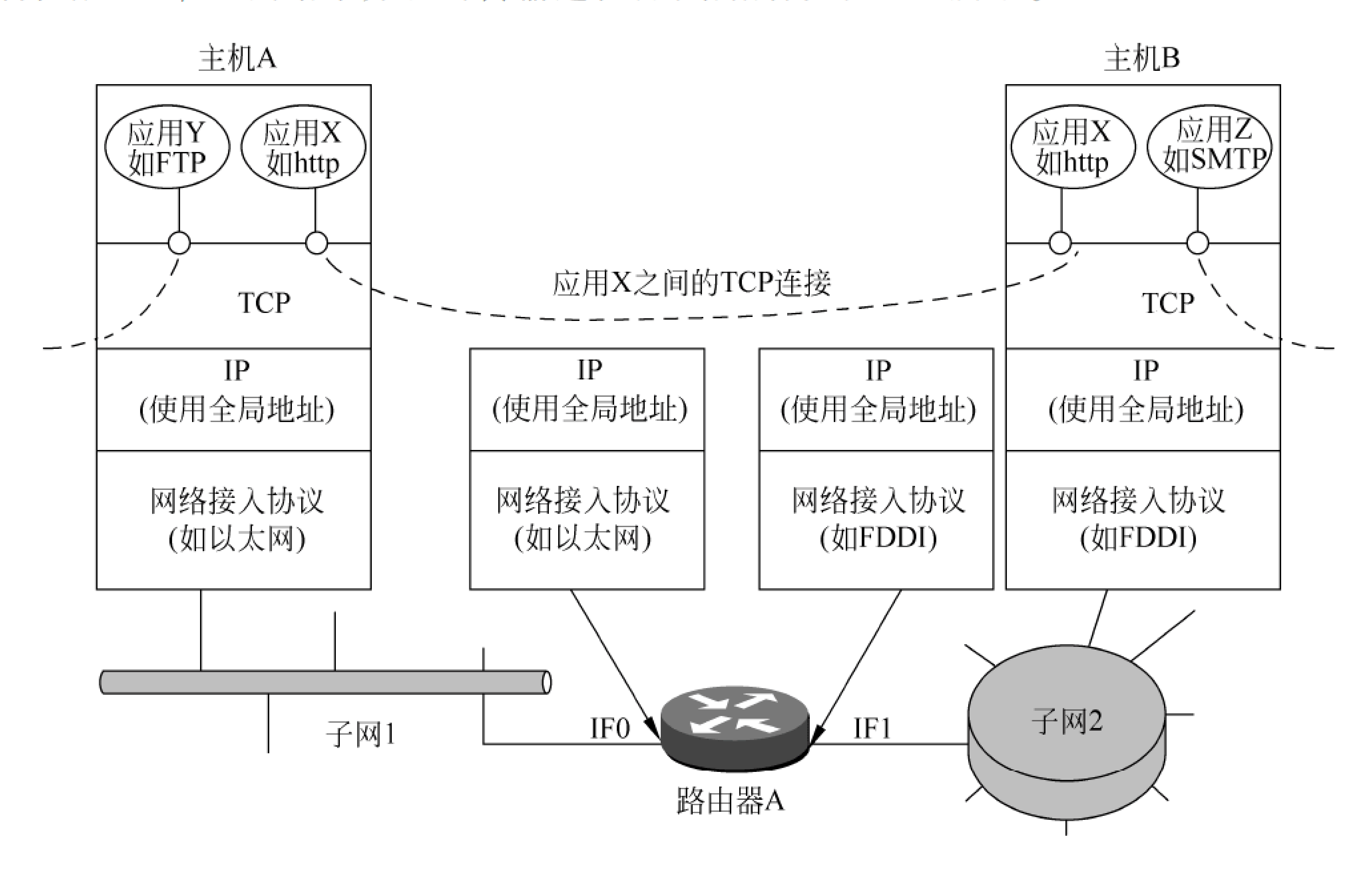


图 5-4　TCP/IP 网络中数据的传输过程

1. 重要概念

在如图 5-4 所示的通信过程中，涉及到一些关键技术和概念。为便于对操作过程的描述，下面对一些重要概念进行简要介绍。

(1) 子网。一个大型的通信网络由多个子网(Subnetwork)组成，每一个子网属于某一种特定类型的网络，如局域网中的以太网、令牌环网、FDDI，广域网中的 X.25、帧中继等。不同子网之间一般需要路由器进行连接，由路由器负责 IP 分组在不同子网之间的转发。

(2) 网络接入协议。当计算机接入网络中时，必须使用这一子网中规定的接入协议。通过网络接入协议，可以让一台主机将数据通过子网发送到其他的主机。例如，当计算机接入以太网时，就需要使用以太网的接入协议，通过主机的 MAC 地址进行数据的转发。

(3) 路由器。它是连接不同子网的设备，一台路由器相当于一个中继站，将一个 IP 分组从某一子网中的一台主机通过一个或多个子网发送到目的主机。路由器转发分组的依据是位于每一台路由器中的路由表。当源主机向目的主机发送数据时，为了保证数据能够正确到达，其首要条件是每一台路由器中的路由表必须是完善的，即在任何一台路由器中都有同一网络中其他子网的路由信息。路由表就好像电话查号台的电话号码簿，如果要保证能够通过查号台查到用户需要的电话，前提条件是电话号码簿中的记录是完整的。路由器工作在 TCP/IP 参考模型的网际层。

(4) 全局地址。对于 Internet 等互联网络来说，每一台主机必须拥有一个全网唯一的 IP 地址作为其身份的唯一标识，这个 IP 地址称为全局地址。当源主机发送数据到目的主机时，源主机首先要知道目的主机的 IP 地址。

（5）端口。主机中的每一个进程必须具有一个在本主机中唯一的地址，这个地址称为端口(port)。通过端口，端到端的协议(如TCP)才能够将数据正确地交付给相应的进程。IP地址确定了网络中唯一的一台主机，而端口确定了主机中唯一的一个进程。

2. 操作过程

如图5-4所示，下面简要描述主机A与主机B进程之间的通信过程，即数据在主机A与主机B之间的转发过程，通信中假设使用了TCP协议。主要过程如下。

（1）假设主机A中的某一个应用程序(进程)要向主机B发送数据，这时主机A中的这个进程将在本机中获得一个端口，之后这个进程就使用这个确定的端口进行通信，直到本次通信过程结束该端口便被释放。由于TCP是一个可靠的、面向连接的通信协议，所以在主机A与主机B之间正式传输数据之前，主机B也需要为这一次通信过程建立一个唯一的端口。

（2）主机A上的进程通过端口将字节流(数据)交给TCP协议，TCP协议根据网络中的约定将字节流划分成为字节段，即将大块数据划分成为小块的数据。然后给每一个字节段添加控制信息，即TCP首部，当在字节段上添加了TCP首部后称为TCP报文段。TCP首部主要包括以下内容。

① 目的端口(destination port)。即主机B上对应进程使用的端口，这个端口是在主机A与主机B正式发送数据之前双方协商建立的。主机B在接收到TCP报文段时，根据端口交付给对应的进程。因为主机B除了与主机A之间的这一进程通信之外，还有可能与主机A或其他主机的不同进程之间同时进行通信。

② 序号(sequence number)。根据在字节流中位置的先后顺序给字节段进行编号。编号的目的之一是每一个字节段单独选择自己的路由在网络中传输，目的之二是当某一个字节段在传输过程中丢失或出错时，接收方可以让发送方重传该字节段，而不需要重传整个字节流。

③ 检验和(checksum)。检验和是对每一个字节段(不是报文段，因为不包括TCP首部)利用某一函数运行产生的值。当接收端(主机B)接收到该字节段时，也会使用相同的函数进行运算，并将运算值与检验和进行比较。如果相同，说明该字节段在传输过程中没有出错；否则需要让对方进行重传。

（3）主机A将TCP报文段下传给IP，并要求它将数据发送到主机B。这时主机A会添加一个IP首部，IP首部包括了源主机(主机A)的IP地址和目的主机(主机B)的IP地址。添加了IP首部的数据称为IP数据报或IP分组。

（4）当IP分组到达网络接口层时，网络接口层又加上自己的首部，即网络首部，这时数据进入了第一个子网(子网1)。网络首部根据接入网络类型的不同而不同，如以太网、令牌环和FDDI等。但在网络首部中一般要包含以下的内容。

① 目的子网地址。子网必须知道应将数据帧发送给哪一个相连设备，如路由器A上物理接口IF0的物理地址。

② 设施请求。网络接入协议可能会请求使用特定的子网设施，如优先级等。

将添加了网络首部的数据单元称为网络级分组或数据帧。

（5）数据帧到了路由器A后，首先被去掉网络首部，得到IP数据报，并根据IP首部的信息知道目的主机的IP地址。然后在路由表中查询该IP地址，如果找到对应的表项，则根

据表项中的信息(其中主要包括路由器上对应的物理接口,如 IF1)将该 IP 数据报转发出去。为了实现这一过程,在路由器 A 上还需要根据下一子网的类型添加网络首部。如果网络中存在多个子网,连接不同子网的路由器都要进行类似于路由器 A 的操作。

(6) 当数据到达主机 B 后,其操作过程与主机 A 的正好相反。在每一层都要去掉相应的首部,并进行相应的约定操作(如检验等),然后将数据交付给上层,直到将原始数据(字节流)交付给指定的进程。

在 TCP/IP 参考模型中,每一层的数据称为协议数据单元(PDU),例如 TCP 报文段也称为 TCP PDU。在数据发送端,在每一层添加首部信息的过程称为数据封装,如图 5-5 所示。在数据接收端,每一层去掉首部信息的过程称为数据解封。

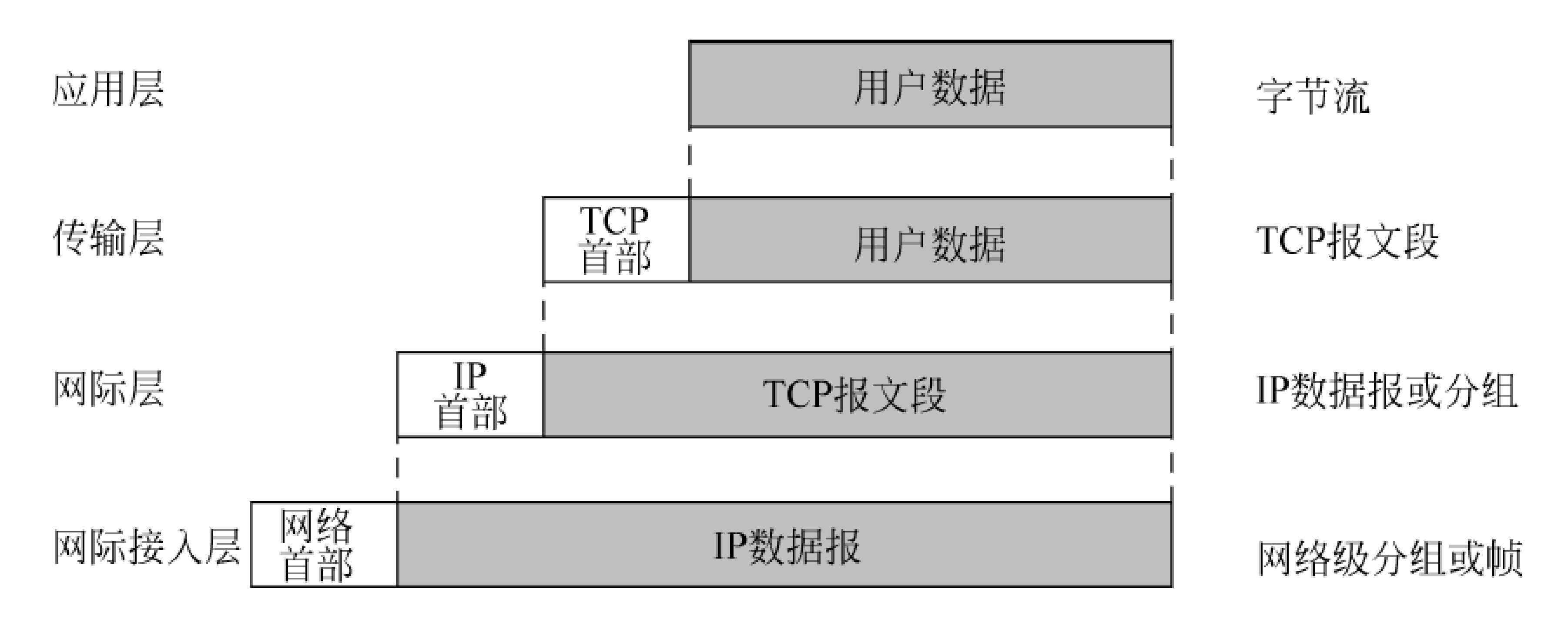


图 5-5　TCP/IP 网络中数据的封装过程

5.2　ARP 安全

ARP(Address Resolution Protocol,地址解析协议)用来将 IP 地址映射到 MAC 地址,以便设备能够在共享介质的网络(如以太网)中通信。

5.2.1　ARP 概述

可以举一个例子很好地说明 ARP 是如何工作的。老师要将一封信交给教室里的某个学生,但是她并不认识这个学生,她只知道这个学生的姓名(IP 地址),于是她对教室里所有的人说:“谁是王××,有你的信!”(ARP 请求),当王××听到这个消息时(地址匹配),他站起来回答,然后老师就知道了他坐在几排几座(MAC 地址),最后把信送到他座位上。

在 ARP 协议的实现中还有一些应该注意的事项。

(1) 每台计算机上都有一个 ARP 缓冲,它保存了一定数量的从 IP 地址到物理地址(MAC 地址)的映射。同时当一个 ARP 广播到来时,虽然这个 ARP 广播可能与它无关,但 ARP 协议软件也会把其中的物理地址与 IP 地址的映射记录下来,这样做的好处是能够减少 ARP 报文在局域网上发送的次数。

(2) 按照默认设置,ARP 高速缓存中的项目是动态的,ARP 缓冲中 IP 地址与物理地址之间的映射并不是一旦生成就永久有效的。每一个 ARP 映射表项都有自己的寿命,如果在一段时间内没有使用,那么这个 ARP 映射就会从缓冲中被删除,这一点和交换机 MAC 地址表的原理一样。这种老化机制,大大减少了 ARP 缓存表的长度,加快了查询速度。

在以太网中,当主机要确定某个 IP 地址的 MAC 地址时,它会先检查自己的 ARP 缓冲表,如果目标地址不包含在该缓冲表中,主机就会发送一个 ARP 请求(广播形式),网段上的任何主机都可以接收到该广播,但是只有目标主机才会响应此 ARP 请求。由于目标主机在收到 ARP 请求时可以学习到发送方的 IP 地址到 MAC 地址的映射,因此它采用一个单播消息来回应请求。这个过程如图 5-6 所示。

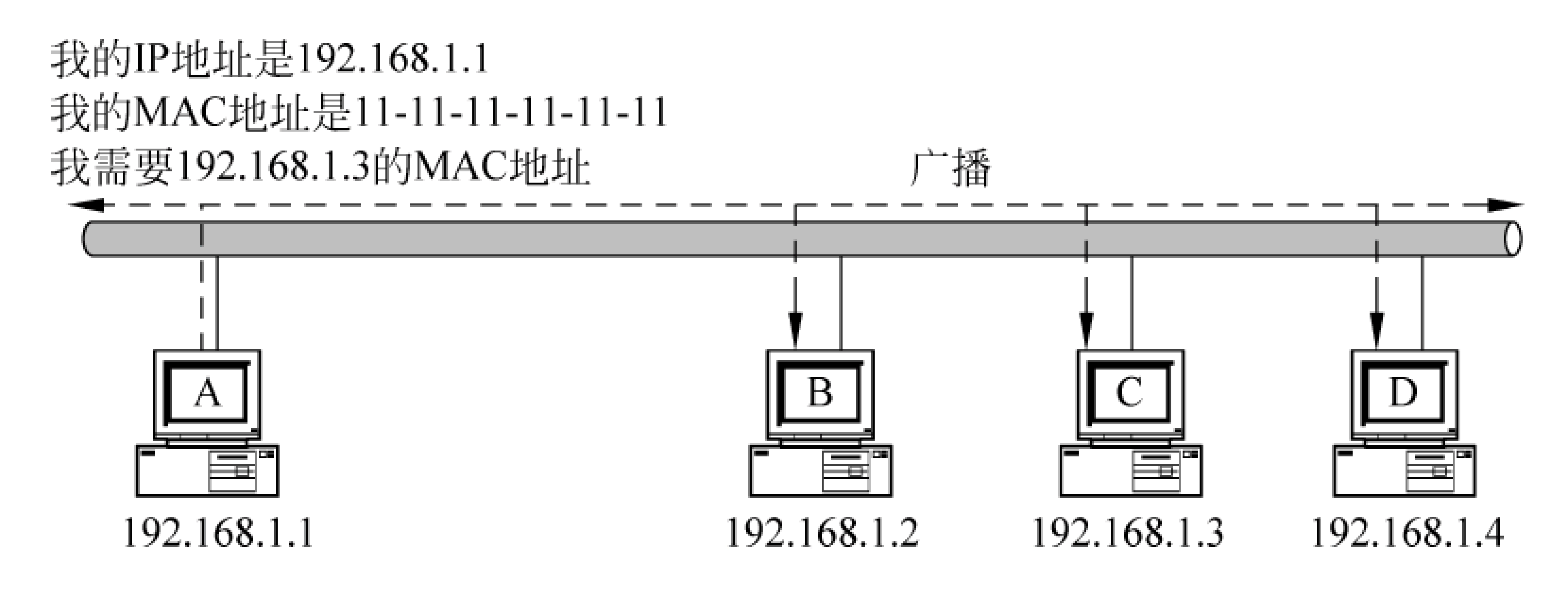


图 5-6　ARP 请求的过程

在图 5-6 中,主机 A 以广播形式发送 ARP 请求查询 IP 地址为 192.168.1.3 的主机的 MAC 地址,网段上所有的主机都会收到该 ARP 请求。

如图 5-7 所示,主机 B、主机 D 收到主机 A 发来的 ARP 请求时,它们发现这个请求不是发给自己的,因此它们忽略这个请求,但是它们还是将主机 A 的 IP 地址到 MAC 地址的映射记录到自己的 ARP 表中。当主机 C 收到主机 A 发来的 ARP 请求时,它发现这个 ARP 请求是发给自己的,于是它用单播消息回应 ARP 请求,同时记录下主机 A 的 IP 地址到 MAC 地址的映射。

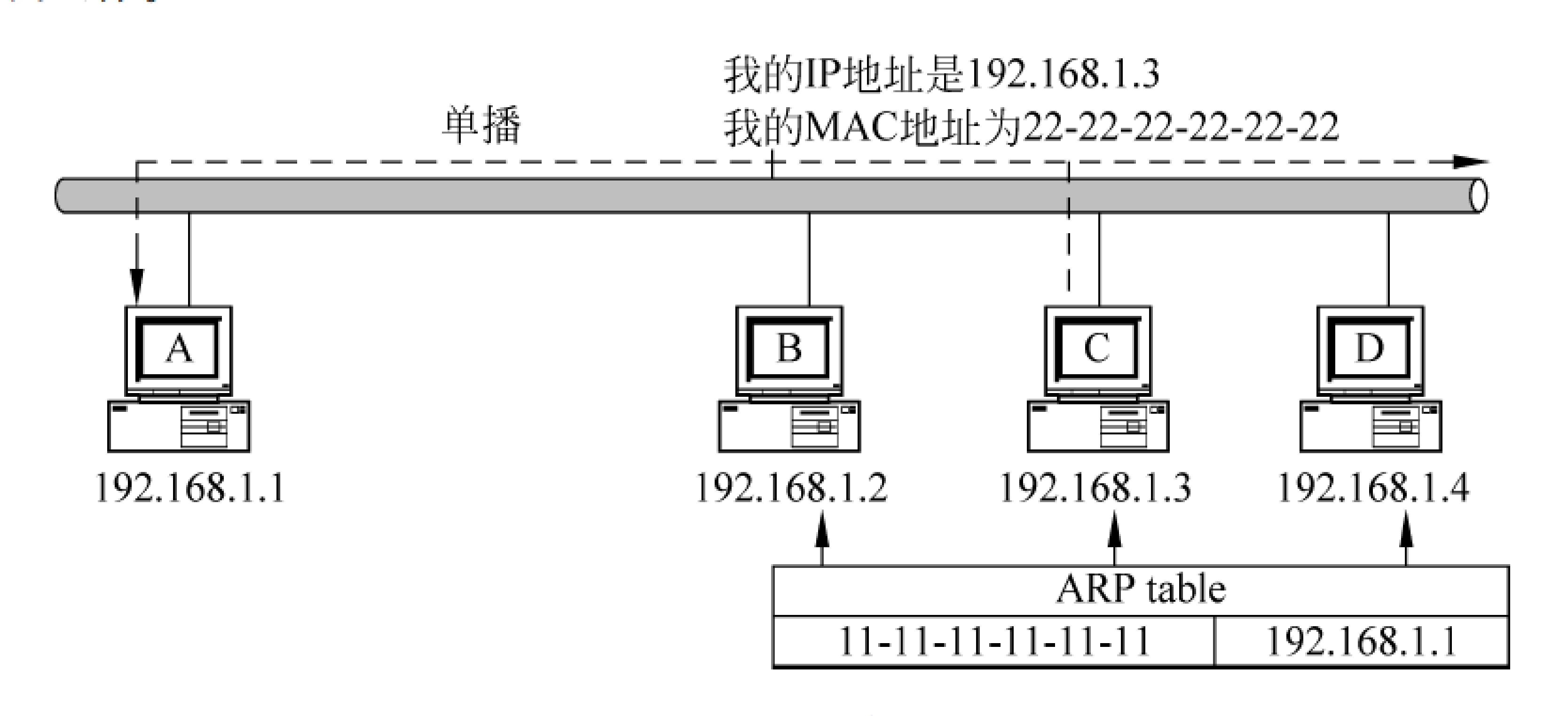


图 5-7　ARP 回应的过程

反向 ARP(Reverse Address Resolution Protocol,RARP)是 ARP 的逆过程,即通过 MAC 地址找到对应的 IP 地址。

5.2.2　ARP 欺骗

通过对 5.2.1 小节内容的学习,读者会发现 ARP 本来是局域网中计算机之间通信时所采用的一种非常有效的协议。但是,由于一台 ARP 主机在给另一台主机发送 ARP 响应时,并不一定首先要得到另一台主机的 ARP 请求,局域网中的任何一台主机都可以给其他主机发送公告:我的 IP 地址是××,我的 MAC 地址是××。这种协议设计上的漏洞便为网络攻击提供了可乘之机。

1. ARP 欺骗的概念和现状

由于 ARP 协议在设计中存在的主动发送 ARP 报文的漏洞，使得主机可以发送虚假的 ARP 请求报文或响应报文，报文中的源 IP 地址和源 MAC 地址均可以进行伪造。在局域网中，即可以伪造成某一台主机（如服务器）的 IP 地址和 MAC 地址的组合，也可以伪造成网关的 IP 地址和 MAC 地址的组合等。这种组合可以根据攻击者的意图进行任意搭配，而现有的局域网中却没有相应的机制和协议来防止这种伪造行为。近几年来，局域网中的 ARP 欺骗已经泛滥成灾，几乎没有一个局域网未遭遇过 ARP 欺骗的侵害。

由于 ARP 协议工作在 TCP/IP 参考模型的网际层与网络接口层之间（OSI 参考模型的网络层与数据链路层之间），所以现有的网管软件和防病毒软件几乎对 ARP 欺骗无能为力，网络管理员只能通过地址绑定等最简单和原始的方法来防御 ARP 欺骗，而缺乏一种行之有效的全网解决方案。

从大量的 ARP 欺骗行为来看，虽然有一部分是为了窃取他人计算机上发送的报文信息，但占的比例并不大。目前，绝大部分 ARP 欺骗是为了扰乱局域网中合法主机中保存的 ARP 表，使得网络中的合法主机无法正常通信或通信不正常，如表现为计算机无法上网或上网时断时续等。ARP 欺骗中的主机是指主要以 MAC 地址作为通信地址的设备，如局域网中的计算机、交换机等。所以，下面将分别针对计算机和交换机来介绍 ARP 欺骗的现象。

2. 针对计算机的 ARP 欺骗

要全面理解 ARP 欺骗，首先要掌握如图 5-3 所示的 TCP/IP 体系结构的工作特点，即明确 ARP 协议在 TCP/IP 参考模型中的位置：网际层与网络接口层之间。目前，局域网中的 ARP 欺骗形式多种多样，下面仅以最常见的一种 ARP 欺骗现象为例进行介绍。

如图 5-8 所示，假设主机 A 向主机 B 发送数据。在主机 A 中，当应用程序要发送的数据到了 TCP/IP 参考模型的网际层与网络接口层之间时，主机 A 在 ARP 缓存表中查找是否有主机 B 的 MAC 地址（其实是主机 B 的 IP 地址与 MAC 地址的对应关系）。如果有，则直接将该 MAC 地址（22-22-22-22-22-22）作为目的 MAC 地址添加到数据单元的网络首部（位于网络接口层），成为数据帧。在局域网（同一 IP 网段，如本例的 192.168.1.x）中，主机利用 MAC 地址作为寻址的依据，所以主机 A 根据主机 B 的 MAC 地址，将数据帧发送给主机 B。

主机	IP 地址	MAC 地址
主机 A	192.168.1.1	11-11-11-11-11-11
主机 B	192.168.1.2	22-22-22-22-22-22
主机 C	192.168.1.3	33-33-33-33-33-33
主机 D	192.168.1.4	44-44-44-44-44-44
主机 E	192.168.1.5	55-55-55-55-55-55

图 5-8　主机中 IP 地址与 MAC 地址的对应关系示意图

如果主机 A 在 ARP 缓存表中没有找到目标主机 B 的 IP 地址对应的 MAC 地址，主机 A 就会在网络上发送一个广播帧，该广播帧的目的 MAC 地址是 FF.FF.FF.FF.FF.FF，表示向局域网内的所有主机发出这样的询问：IP 地址为 192.168.1.2 的 MAC 地址是什么？

在局域网中所有的主机都会接收到该广播帧，但在正常情况下因为只有主机 B 的 IP 地址是 192.168.1.2，所以主机 B 会对该广播帧进行 ARP 响应，即向主机 A 发送一个 ARP 响应帧：我(IP 地址是 192.168.1.2)的 MAC 地址是 22-22-22-22-22-22。

这样，主机 A 就知道了主机 B 的 MAC 地址，它就可以向主机 B 发送数据了。同时主机 A 还会更新自己的 ARP 缓存表，将主机 B 的 IP 地址与 MAC 地址的对应关系保存在自己的 ARP 缓存表中，以供下次通信时直接使用，避免进行广播查询。

但是，主机的 ARP 缓存中并不会保存所有参与过通信的主机的 IP 地址和 MAC 地址的对应关系，而是采用了老化机制防止 ARP 缓存表过于庞大，因为过于庞大的 ARP 缓存表会影响主机的通信效率。在一段时间内，如果 ARP 缓存表中的某一条记录没有使用，就会被删除。

从上面的例子可以看出，ARP 协议的基础就是信任局域网内所有的主机，这样就很容易实现在局域网内的 ARP 欺骗。如果现在主机 D 要对主机 A 进行 ARP 欺骗，冒充自己是主机 C。具体实施中，当主机 A 要与主机 C 进行通信时，主机 D 主动告诉主机 A 自己的 IP 地址和 MAC 地址的组合是 192.168.1.3＋44-44-44-44-44-44，这样当主机 A 要发送给主机 C 数据时，会将主机 D 的 MAC 地址 44-44-44-44-44-44 添加到数据帧的目的 MAC 地址中，从而将本来要发给主机 C 的数据发给了主机 D，实现了 ARP 欺骗。在整个 ARP 欺骗过程中，主机 D 称为"中间人(man in the middle)"，对这一中间人的存在主机 A 根本没有意识到。

通过以上的 ARP 欺骗，使主机 A 与主机 C 之间断开了联系。如图 5-9 所示，现在假设主机 C 是局域网中的网关，而主机 D 为 ARP 欺骗者。这样，当局域网中的计算机要与其他网络进行通信(如访问 Internet)时，所有发往其他网络的数据全部发给了主机 D，而主机 D 并非真正的网关，这样整个网络将无法与其他网络进行通信。这种现象在 ARP 欺骗中非常普遍。

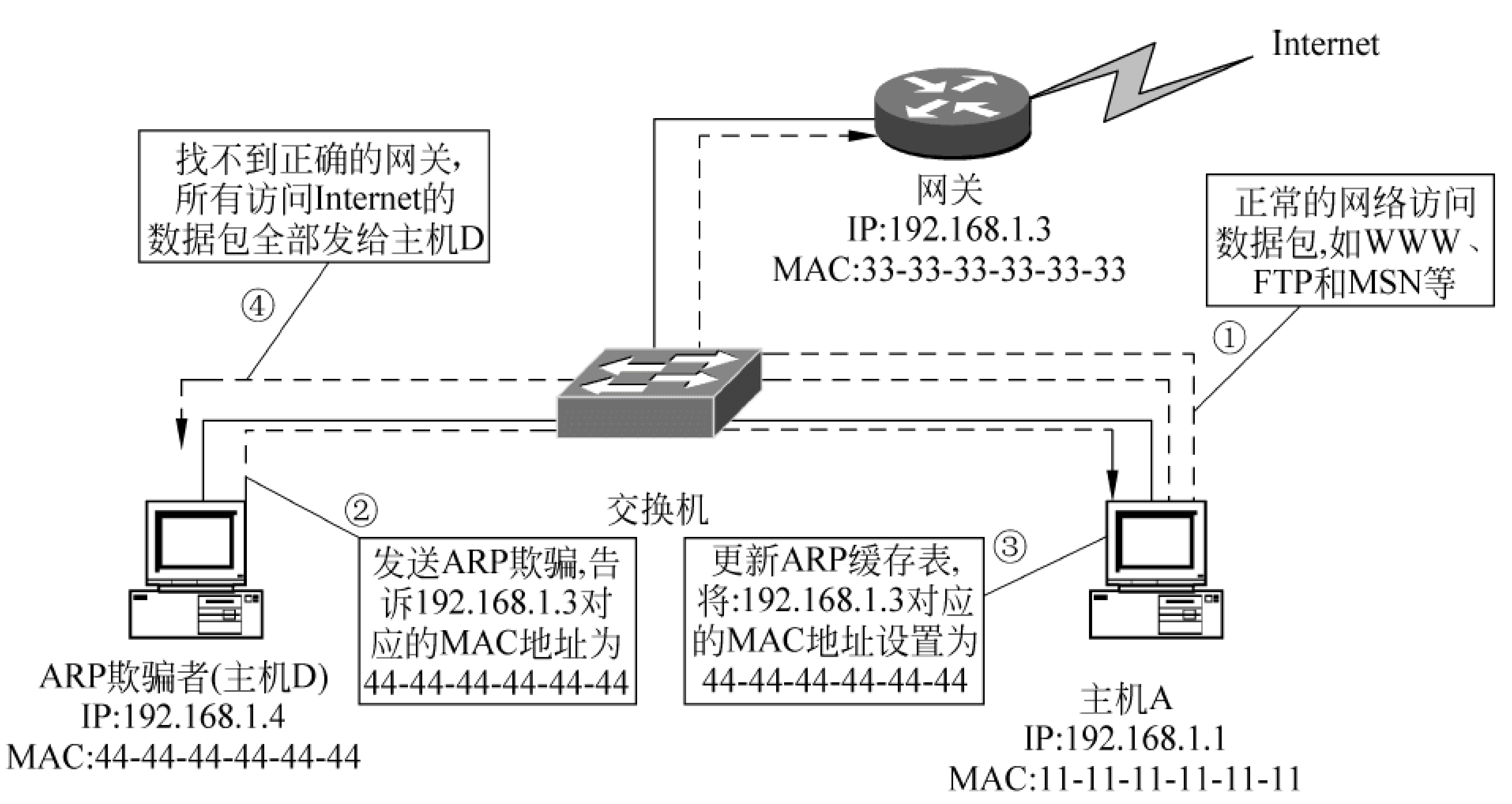


图 5-9　ARP 欺骗的实现过程

3. 针对交换机的 ARP 欺骗

交换机的工作原理是通过主动学习下连设备的 MAC 地址，并建立、维护端口及 MAC 地址的对应表，即交换机中的 MAC 地址表。通过 MAC 地址表，实现下连设备之间的通

信。交换机中的 MAC 地址表也称为 CAM(Content Addressable Memory,内容可寻址存储器),如图 5-10 所示。

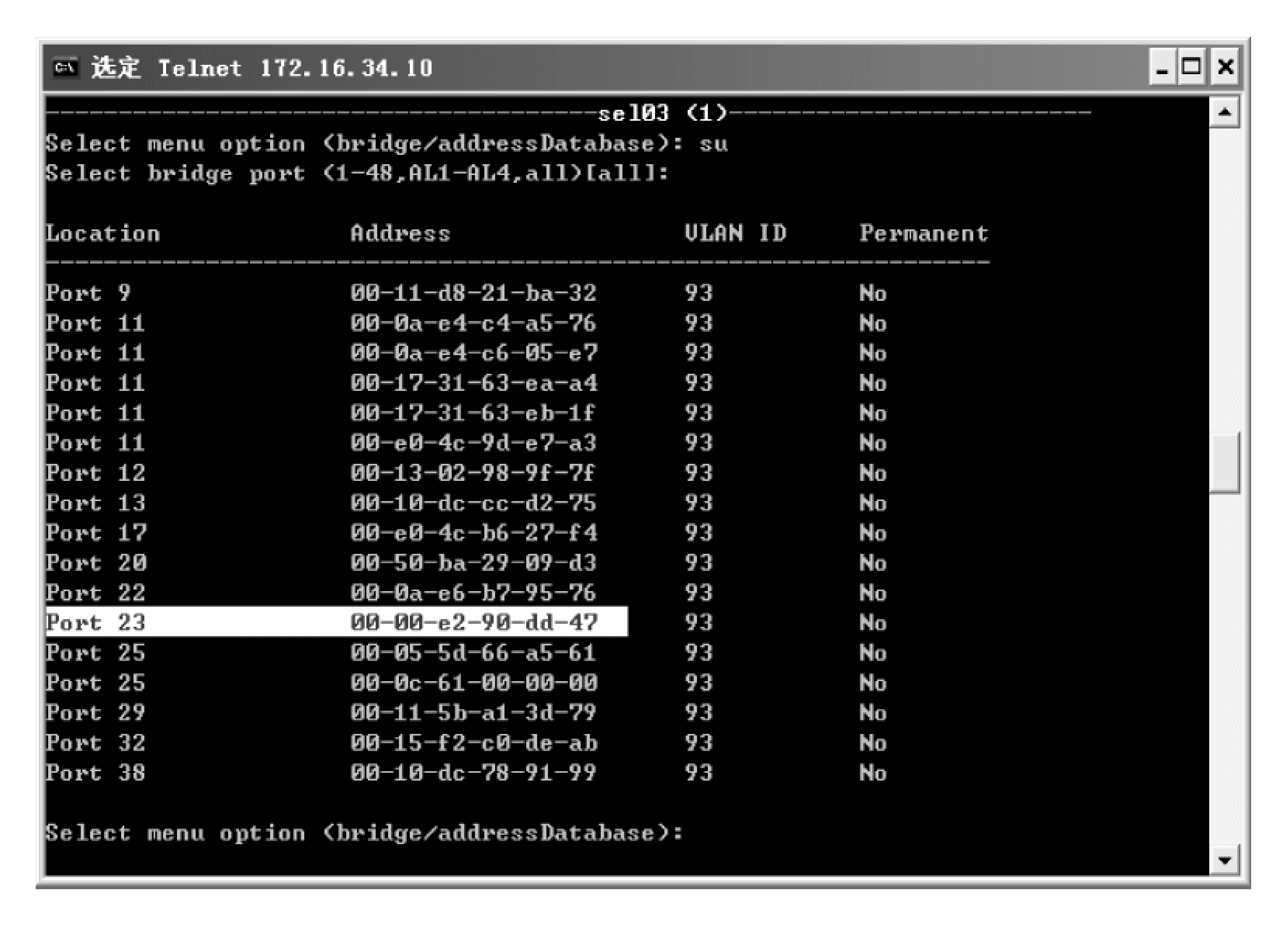


图 5-10 交换机中的 MAC 地址表

交换机中的 CAM 表详细地记录了参与通信的下连设备的 MAC 与交换机端口的一一对应关系。CAM 表在交换机加电启动时是空的,当下连的某一台主机要通信时,交换机会自动将该主机的 MAC 地址与下连端口的对应关系记录下来,在 CAM 表中形成一条记录,将这一过程称为交换机的学习。CAM 表的大小是固定的,不同交换机的 CAM 表大小可能不同。

在进行 ARP 欺骗时,ARP 欺骗者利用工具产生欺骗 MAC,并快速填满 CAM 表。交换机的 CAM 表被填满后,交换机便以广播方式处理通过交换机的数据帧,这时 ARP 欺骗者可以利用各种嗅探攻击获取网络信息。CAM 表被填满后,流量便以洪泛(Flood)方式发送到所有端口,其中交换机上连端口(Trunk 端口)上的流量也会发送给所有端口和邻接交换机。这时的交换机其实已成为一台集线器。与集线器不同,由于交换机上有 CPU 和内存,大量的 ARP 欺骗流量会给交换机产生流量过载,其结果是下连主机的网络速度变慢,并造成数据包丢失,甚至产生网络瘫痪。

在计算机网络中曾经出现的 SQL 蠕虫病毒就是利用组播功能,构造虚假的目的 MAC 地址将交换机的 CAM 表填满,对网络安全运行造成了非常大的威胁。

5.2.3 实验操作 1 ARP 欺骗的防范

由于 ARP 欺骗方式多种多样,所以对 ARP 欺骗的防范方法也不尽相同。下面以上文介绍的针对计算机的 ARP 欺骗和针对交换机的 ARP 欺骗为例,分别介绍与之对应的防范方法。

1. 针对计算机 ARP 欺骗的防范

ARP 缓存表中的记录可以是动态的(基于前面介绍的 ARP 响应),也可以是静态的。如果 ARP 缓存表中的记录是动态的,即为了减少 ARP 缓存表的长度,加快查询速度,ARP

缓存表采用了老化机制，在一段时间内如果表中的某一条记录没有使用就会被删除。其中，Windows 操作系统的老化时间默认为 2 分钟，而 Cisco 路由器老化时间默认为 5 分钟。

静态 ARP 缓存表中的记录是永久性的，用户可以使用 TCP/IP 工具来创建和修改，如 Windows 操作系统自带的 ARP 工具。下面用类似于图 5-9 所示的网络环境，以 Windows 操作系统为例，通过在用户计算机上绑定网关的 IP 地址和 MAC 地址的方法来防范出现网关地址的 ARP 欺骗。具体操作如下。

（1）进入“命令提示符”窗口，在确保网络连接正常的情况下，使用 Ping 命令 Ping 网关的 IP 地址，如 Ping 172.16.2.1。

（2）在保证 Ping 网关 IP 地址正常的情况下，输入 arp-a 命令，可以获得网关 IP 地址对应的 MAC 地址，如图 5-11 所示。

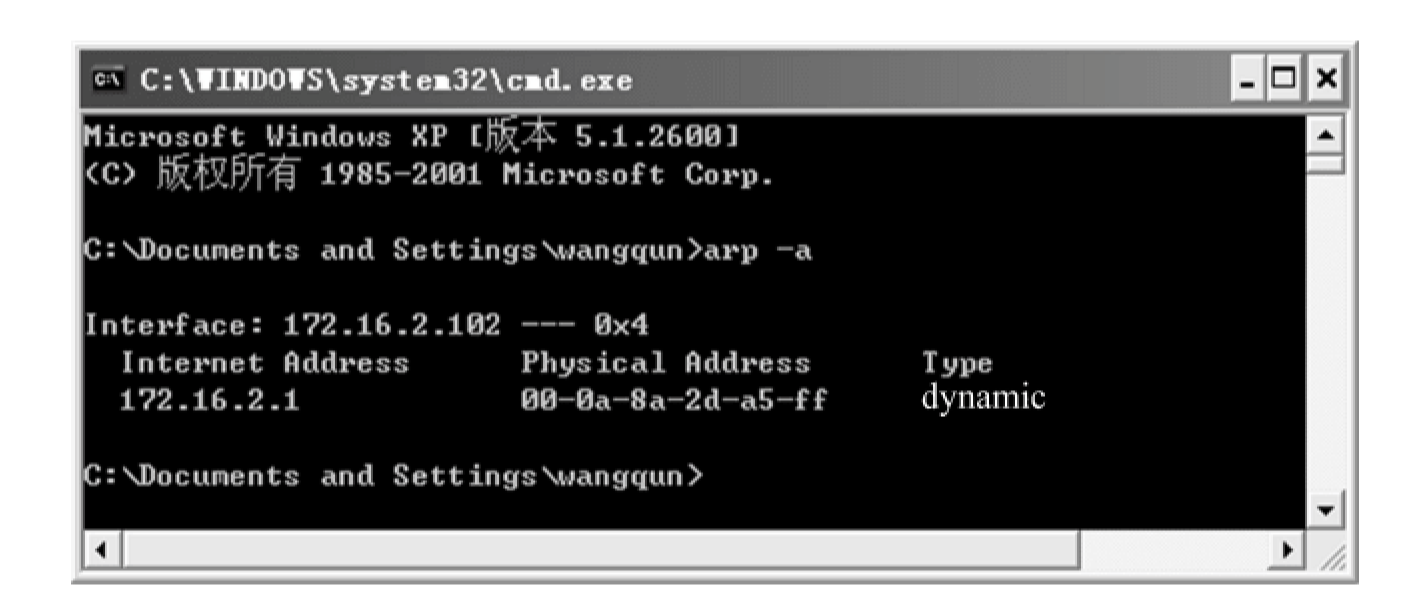


图 5-11　使用 arp-a 命令显示网关 IP 地址对应的 MAC 地址

读者会发现，这时该计算机上网关对应的 ARP 记录类型是动态的。

（3）利用“arp-s 网关 IP 地址 网关 MAC 地址”将本机中 ARP 缓存表中网关的记录类型设置为静态，如图 5-12 所示。



图 5-12　将 ARP 缓存中的网关记录设置为静态类型

（4）如果再次输入 arp-a 命令，就会发现 ARP 缓存表中网关的记录已被设置为静态类型。

以上操作仅适用于实验环境，因为利用以上手工设置方式修改的 ARP 缓存表中的记录，会在计算机重新启动后失效，需要再次绑定。这显然在实际的网络环境中是不适用的。为解决这一问题，针对以上操作，可以编写一个批处理文件（如 arp.bat），然后将该批处理文件添加到 Windows 操作系统的“启动”栏中，这样每次开机后系统便会进行自动绑定。批处理文件的内容如下。

```
@echo off
arp-d
arp-s 172.16.2.1 00-0a-8a-2d-a5-ff
```

以上介绍是针对网关进行的设置。如果用户的计算机需要经常与另一台计算机之间进行可靠的通信,则可以将对方计算机的 ARP 记录以静态方式添加到本机的 ARP 缓存表中。

2. 针对交换机 ARP 欺骗的防范

在交换机上防范 ARP 欺骗的方法与在计算机上防范 ARP 欺骗的方法基本相同,还是使用将下连设备的 MAC 地址与交换机端口进行一一绑定的方法来实现。在不同交换机上实现地址绑定的操作方法可能不同,Cisco 系列交换机上实现地址绑定的操作方法可参看本书第 4 章的 4.3.1 节的内容。

目前,主流的交换机(如 Cisco、H3C 和 3COM 等)都提供了端口安全功能(Port Security feature)。通过使用端口安全功能,可以进行如下的控制。

(1) 端口上最大可以通过的 MAC 地址数量。

(2) 端口上只能使用指定的 MAC 地址。

对于不符合以上规定的 MAC 地址,进行相应的违背规则的处理。一般有如下三种方式(针对交换机类型和型号的不同,具体方式可能会有所不同)。

(1) Shutdown。即关闭端口。虽然这种方式是最有效的一种保护方式,但会给管理员带来许多不便,因为被关闭的端口一般需要通过手工方式进行重启。

(2) Protect。直接丢弃非法流量,但不报警。

(3) Restrict。丢弃非法流量,且产生报警。

通过利用端口安全功能,可以防范交换机 MAC/CAM 攻击。下面以 Cisco 系列交换机为例进行介绍,其他交换机的配置原理与此基本相同,具体的配置命令可参阅相关的技术文档。

在进行端口安全功能设置时,端口上的 MAC 地址既可以通过交换机的自动学习功能获得,也可以通过手工方式进行 MAC 地址与端口的绑定。当通过自动学习功能获得 MAC 地址时,交换机重启后会主动学习下连端口设备的 MAC 地址,直到学习到的 MAC 地址数达到设置的数量。但是,当交换机关机或重启后又要进行重新学习。下面以交换机的端口 fastethernet0/1 为例,通过手工方式进行 MAC 地址与端口的绑定,介绍端口安全的配置方法。

```
Switch #conf t (进入配置模式)
Switch(config) #interface fastethernet0/1 (选择 fastethernet0/1 端口,进入该端口配置状态)
Switch(config-if) #switchport port-security maximum 2 (设置最大 MAC 地址数为 2)
Switch(config-if) # switchport port-security violation shutdown (当违背安全规则后自动关闭
端口)
Switch(config-if) #end (退出配置模式)
Switch #wr (保存设置)
```

目前较新的端口安全技术是 Sticky Port Security,它克服了 Port Security feature 存在的交换机重启后 CAM 表中自动学习获得的 MAC 地址会丢失的不足,交换机可以将学到的 MAC 地址写入到端口配置中,即使交换机重启或关机,配置仍然存在。

还需要说明的是,由于 ARP 欺骗的严重性,许多交换机设备制造商纷纷推出了可以防范 ARP 欺骗功能的交换机产品。这些产品的效果确实不错,但有一个前提是该网络中所有的交换机都必须使用同一个厂商的产品,而且对交换机的型号也有一定的要求,有些早期的交换机可能无法支持此功能。

5.3 DHCP 安 全

DHCP(Dynamic Host Configuration Protocol,动态主机配置协议)是一个客户机/服务器协议,在 TCP/IP 网络中对客户机动态分配和管理 IP 地址等配置信息,以简化网络配置,方便用户使用及管理员的管理。

5.3.1 DHCP 概述

一台 DHCP 服务器可以是一台运行 Windows Server 2000/2003/2008、UNIX 或 Linux 的计算机,也可以是一台路由器或交换机。DHCP 的工作过程如图 5-13 所示。具体操作过程如下。

(1) DHCP 客户端首次初始化时会向 DHCP 服务器发送一个请求(DHCPDISCOVER),请求获得 IP 寻址信息,这个寻址信息包括 IP 地址、子网掩码、默认网关和 DNS 服务器地址等,请求中同时也包含了客户机自己的 MAC 地址信息。DHCPDISCOVER 以广播形式发送,网段上的所有设备都会收到这个请求。

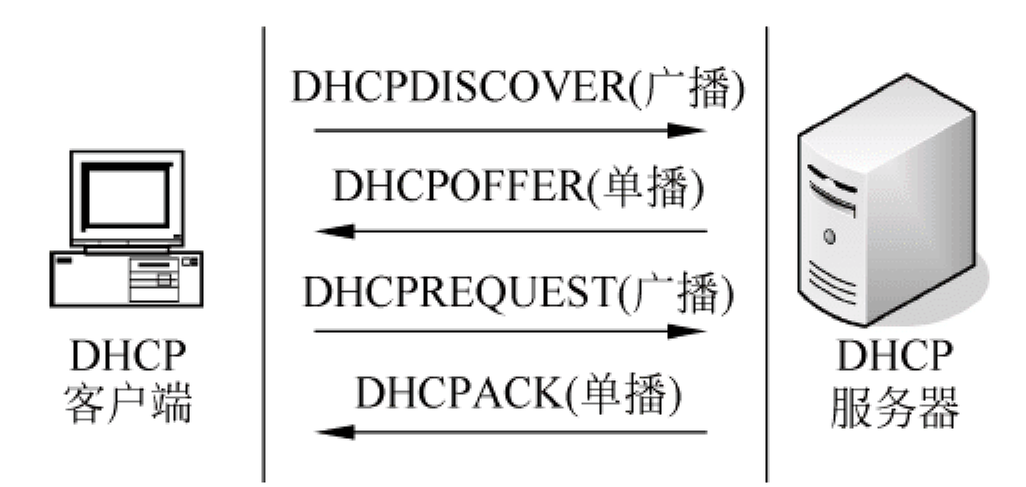


图 5-13　DHCP 的工作过程

(2) 当 DHCP 服务器接收到请求时,它会从自己的地址池中选择一个 IP 地址分配给客户机,并且把其他 TCP/IP 配置一起发送过去(DHCPOFFER)。DHCPOFFER 以单播形式发送,因为它是针对某个具体主机的消息,DHCP 服务器可以从 DHCPDISCOVER 消息中获得客户机的 MAC 地址。

(3) 当客户端接收到服务器所提供的信息时,它又以广播方式发送一个 DHCPREQUEST 消息,指明我需要得到你的服务。

需要注意的是,为什么还要以广播形式发送 DHCPREQUEST 消息呢? 如果一个网段上存在多个 DHCP 服务器,那么 DHCP 客户端可能会收到多个 DHCP 服务器响应的 DHCPOFFER 消息,DHCP 客户端只会选择最先收到的那个 DHCPOFFER 消息。所以,以广播方式发送 DHCPREQUEST 消息有两个作用。一是通知那个服务器:我已经收到你所提供的 IP 地址,我需要你的服务;二是通知网络上其他 DHCP 服务器:我拒绝你们提供的 IP 寻址信息。

(4) DHCP 服务器接收到 DHCPREQUEST 消息后,它会将所提供的 IP 地址和其他设置交给数据库,并且向 DHCP 客户端以单播形式发送一个 DHCPACK 消息,确认 DHCP 过程已经完成。

经过以上几个步骤,这个 IP 地址就会租给这个客户端一段时间,在租用期间,客户端每次登录时都会向服务器发出这个 IP 地址的续定请求(DHCPREQUEST)。如果租用期到了,但是客户端没有续租,这个 IP 地址就会退回到 DHCP 服务器的地址池中等待重新分配。

5.3.2 DHCP 的安全问题

在通过 DHCP 提供客户端 IP 地址等信息分配的网络中存在着一个非常大的安全隐患:当一台运行有 DHCP 客户端程序的计算机连接到网络中时,即使是一个没有权限使用

网络的非法用户也能很容易地从 DHCP 服务器获得一个 IP 地址及网关、DNS 等信息，成为网络的合法使用者。由于在 TCP/IP 网络中，很多权限是基于 IP 地址来设置的，与设备的 MAC 地址不同的是 IP 地址属于逻辑地址，IP 地址具有不确定性，所以如果要进行基于 IP 的认证或权限控制是没有意义的(此问题已在本书第 4 章进行了讨论)。

由于 DHCP 客户端在获得 DHCP 服务器的 IP 地址等信息时，系统没有提供对合法 DHCP 服务器的认证，所以 DHCP 客户端从首先得到 DHCP 响应(DHCPOFFER)的 DHCP 服务器处获得 IP 地址等信息。为此，不管是人为的网络攻击或破坏，还是无意的操作，一旦在网络中接入了一台 DHCP 服务器，该 DHCP 服务器就可以为 DHCP 客户端提供 IP 地址等信息的服务。其结果是客户端从非法 DHCP 服务器获得了不正确的 IP 地址、网关和 DNS 等参数，无法实现正常的网络连接；或客户端从非法 DHCP 服务器处获得的 IP 地址与网络中正常用户使用的 IP 地址冲突，影响了网络的正常运行。尤其是当客户端获得的 IP 地址与网络中某些重要服务器的 IP 地址冲突时，整个网络将处于混乱状态。

如图 5-14 所示，一台非法 DHCP 服务器接入到了网络中，并冒充为这个网段中的合法 DHCP 服务器。这时，如果有一台 DHCP 客户端接入到网络，将向网络中广播一个 DHCPDISCOVER 的请求信息，由于非法 DHCP 服务器与 DHCP 客户端处于同一个网段，而正确的 DHCP 服务器位于其他网段，所以一般情况下非法 DHCP 服务器优先发送 DHCPOFFER 响应给 DHCP 客户端，而后到的正确的 DHCP 服务器的 DHCPOFFER 响应 DHCP 客户端并不采用。这样，DHCP 客户端将从非法 DHCP 服务器处获得不正确的 IP 地址、网关和 DNS 等配置参数。

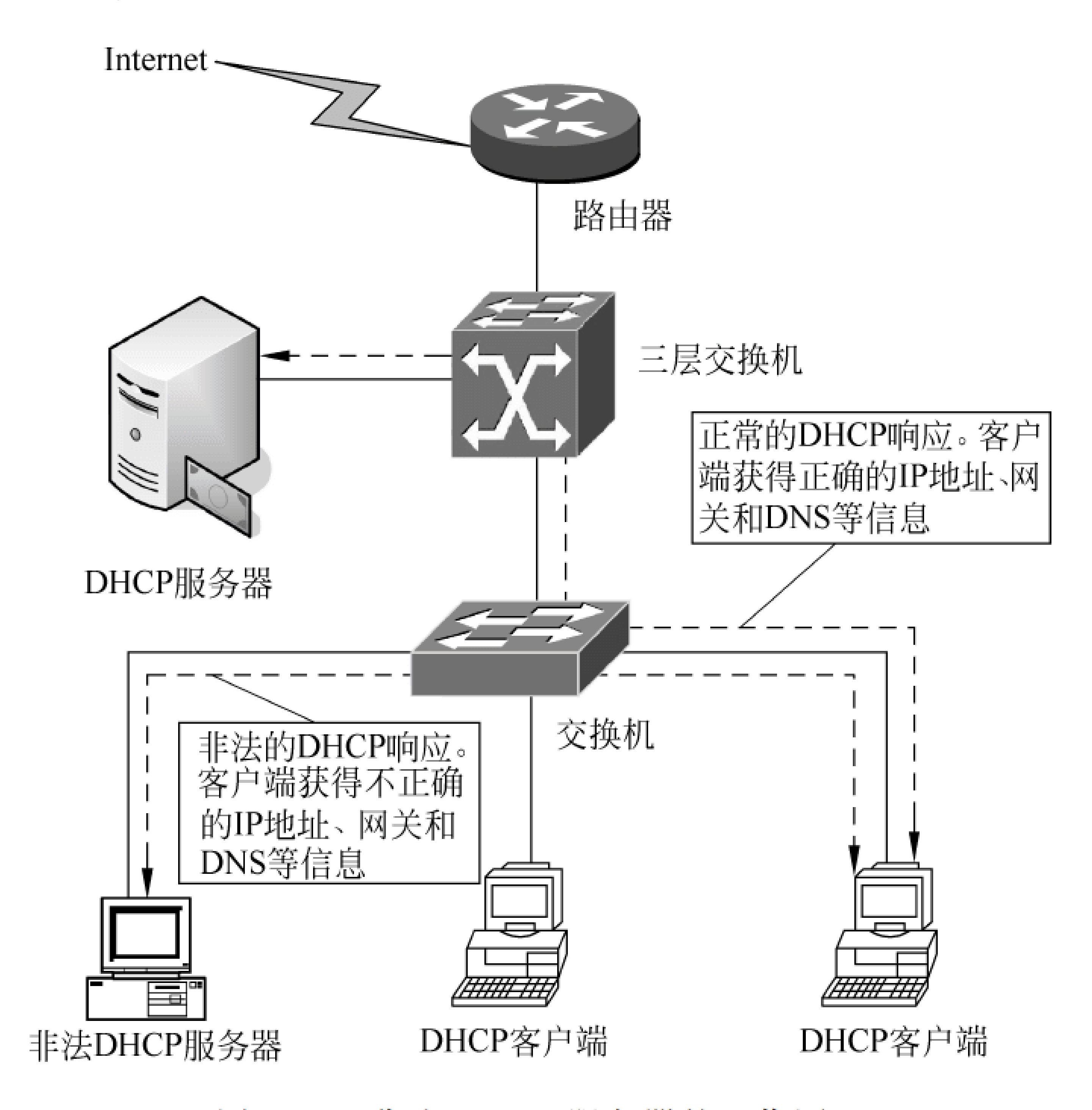


图 5-14　非法 DHCP 服务器的工作原理

5.3.3 实验操作 2 非法 DHCP 服务的防范

非法 DHCP 服务存在大量的安全隐患，如果将非法 DHCP 服务器与一些攻击程序结合使用，则可以很方便地获得网络中用户的有用信息，如操作系统的用户账户和密码等。本节将结合应用实际，介绍几种防范非法 DHCP 服务的有效方法。

1. 使用 DHCP Snooping 信任端口

DHCP Snooping 能够过滤来自网络中非法 DHCP 服务器或其他设备的非信任 DHCP 响应报文。在交换机上，当某一端口设置为非信任端口时，可以限制客户端特定的 IP 地址、MAC 地址或 VLAN ID 等报文通过。为此，可以使用 DHCP Snooping 特性中的可信任端口来防止用户私置 DHCP 服务器或 DHCP 代理。一旦将交换机的某一端口设置为指向正确 DHCP 服务器的接入端口，则交换机会自动丢失从其他端口上接收到的 DHCP 响应报文，如图 5-15 所示。

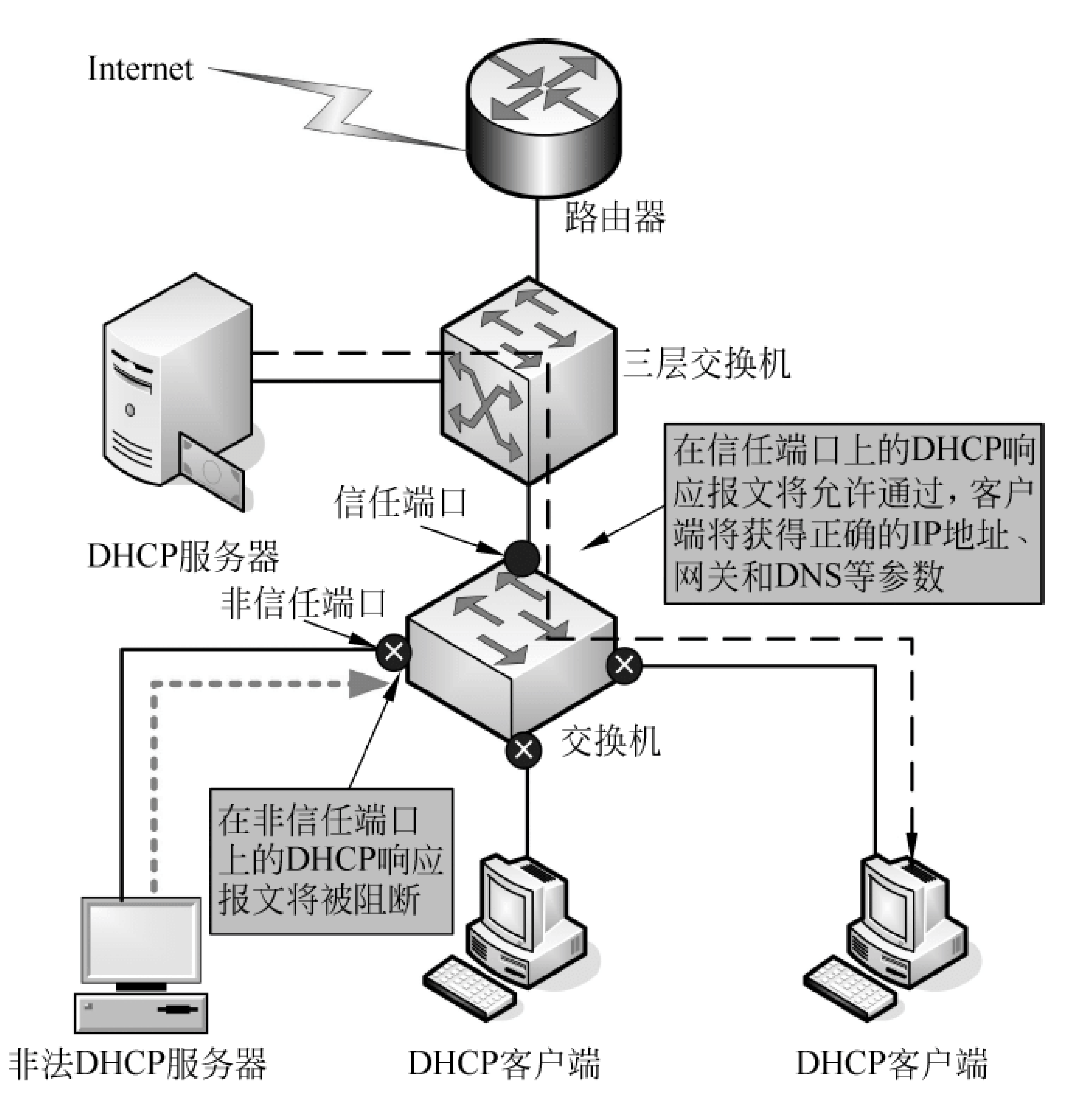


图 5-15 DHCP Snooping 的工作原理

在配置时，可将交换机上与 DHCP 服务器连接的端口设置为 DHCP Snooping 的信任端口，其他端口默认情况下都为非信任端口。在图 5-15 所示的网络中，DHCP 客户端发出 DHCPDISCOVER 请求报文，由于非信任端口并不限制该请求报文，所以非法 DHCP 服务器也会接收到该请求并发送 DHCPOFFER 响应报文。但是，非信任端口会阻断 DHCPOFFER 响应报文的通过，所以 DHCP 客户端只能接收到正确的 DHCP 服务器的响应，避免了非法 DHCP 服务器提供 IP 地址等信息给客户端。

下面介绍在 Cisco 交换机上 DHCP Snooping 特性的实现方法。现在，假设要将交换机的第一个端口 fastethernet0/1 设置为信任端口，DHCP 服务器将连接在该端口上。具体配置方法如下。

```
Switch #conf t  (进入配置模式)
Switch(config) #interface fastethernet0/1  (选择 fastethernet0/1 端口,进入该端口配置状态)
Switch(config-if) # ip dhcp snooping trust  (将该端口设置为受信任端口)
Switch(config-if) # ip dhcp snooping limit rate 500  (设置每秒钟最多处理 500 个 DHCP 报文)
Switch(config-if) #end
Switch #wr
Switch #sh ip dhcp snooping  (显示交换机上 DHCP Snooping 的配置情况)
```

2. 在 DHCP 服务器上进行 IP 与 MAC 地址的绑定

在通过 DHCP 服务器进行客户端 IP 地址等参数分配的网络中,对于一些重要部门的用户,可以通过在 DHCP 服务器上绑定 IP 与 MAC 地址,实现对指定计算机 IP 地址的安全分配。下面以 Windows Server 2003 操作系统集成的 DHCP 服务为例,介绍实现方法。

(1) 确保 DHCP 服务器的运行正常。如果读者的计算机上还没有安装 DHCP 服务器,可通过选择"开始"→"设置"→"控制面板"→"添加或删除程序"→"添加/删除 Windows 组件"→"网络服务"→"详细信息"→"动态主机配置协议(DHCP)"来安装。安装好 DHCP 组件后,还要通过"新建作用域"指定为客户端分配的 IP 地址段、网关和 DNS 等信息。

(2) 选择"开始"→"程序"→"管理工具"→DHCP,打开 DHCP 窗口。

(3) 选取"作用域"→"保留",单击鼠标右键,在弹出的快捷菜单中选择"新建保留"命令,打开如图 5-16 所示的"新建保留"对话框。在"保留名称"文本框中输入客户端用户的名称,在"IP 地址"文本框中输入该作用域中一个未分配的 IP 地址,在"MAC 地址"文本框中输入指定客户端计算机的 MAC 地址,在"支持的类型"选项区域中选择"两者"或"仅 DHCP"单选按钮。

(4) 单击"添加"按钮,完成对该客户端 IP 地址与 MAC 地址的绑定操作。

采用相同的方法,完成对其他 DHCP 客户端 IP 地址与 MAC 地址的绑定操作,最后如图 5-17 所示。

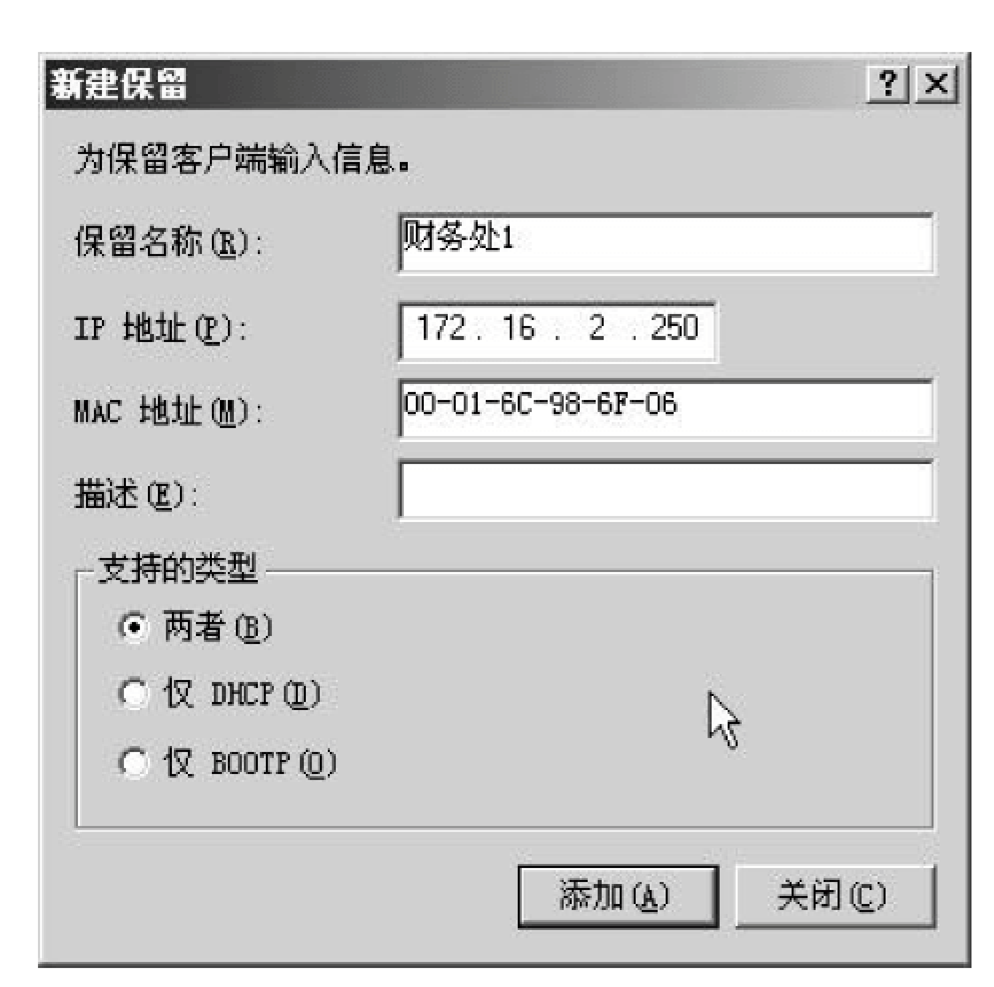


图 5-16 进行 IP 地址与客户端 MAC 地址的绑定



图 5-17 显示已创建的客户端 IP 与 MAC 地址的绑定关系

加强对网络中 DHCP 服务器的安全管理,可以防止出现 DHCP 攻击或欺骗。针对网络中所使用的交换机等设备和 DHCP 服务器软件的不同,所采取的安全技术和策略也不尽相同。读者可通过参阅相关设备和软件的技术文档,加强对 DHCP 服务的管理。

5.4 TCP 安全

UDP 和 TCP 是 TCP/IP 参考模型传输层的两个通信协议。其中,UDP 是一种不可靠的、面向非连接的通信协议,而 TCP 是一种可靠的、面向连接的通信协议。将通过 UDP 协议传输的数据单位称为数据报,而将通过 TCP 协议传输的数据单位称为报文段。由于两种协议的功能不同,所以传输层 UDP 的首部格式非常简单,而 TCP 的首部格式非常复杂。与 UDP 不同的是,TCP 是为可靠的通信过程而开发的协议,但在实际应用中却出现了针对 TCP 协议漏洞的不安全因素,甚至是网络攻击。

5.4.1 TCP 概述

TCP 协议涉及到 TCP 报文段的结构、TCP 连接的建立与终止、TCP 数据的传输、流量控制、差错控制和数据重传等内容。由于本章主要讨论的是协议的安全问题,所以在这里仅关注 TCP 面向连接的传输所需要的三个阶段:连接建立、数据传输和连接终止,对其工作过程进行介绍,并发现存在的安全问题。

1. 连接建立

TCP 是面向连接的。在面向连接的环境中,开始传输数据之前,在两个终端之间必须先建立一个连接。建立连接的过程可以确保通信双方在发送用户数据之前已经准备好了传送和接收数据。对于一个要建立的连接,通信双方必须用彼此的初始化序列号 SEQ 和来自对方成功传输确认的确认序号 ACK 同步(ACK 号指明希望收到的下一个字节的编号)。习惯上将同步信号写为 SYN,应答信号写为 ACK。整个同步的过程称为三次握手,图 5-18 说明了这个过程,具体如下。

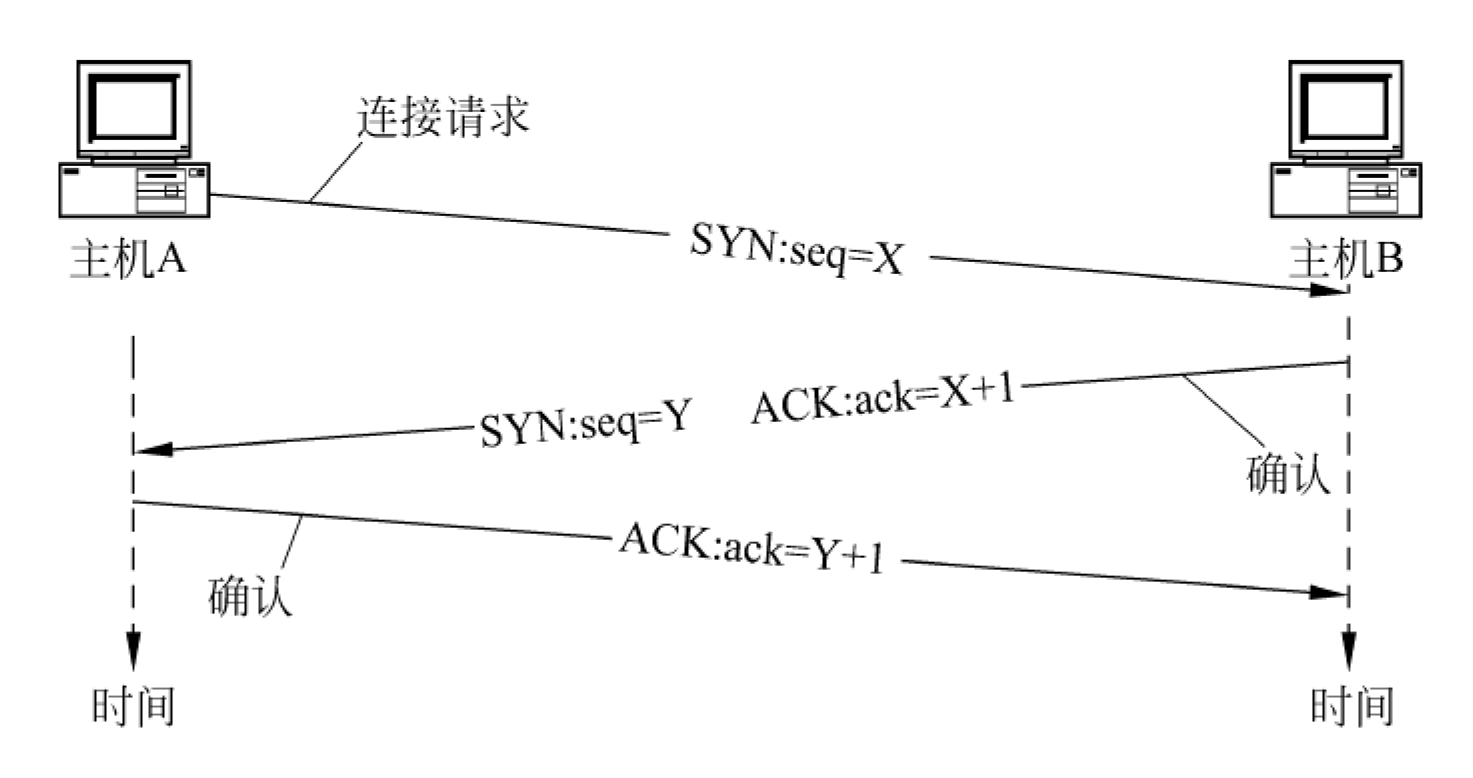


图 5-18　TCP 连接建立时的三次握手

(1) 主机 A 发送 SYN 给主机 B:我的初始化序列号 seq 是 X。主机 A 通过向主机 B 发送 SYS 报文段,实现从主机 A 到主机 B 的序列号的同步,即确定 seq 中的 X。

(2) 主机 B 发送 SYN、ACK 给主机 A:我的初始化序列号 seq 是 Y(如果主机 B 同意与主机 A 建立连接时),确认序号 ack 是 X+1(等待接收第 X+1 号字节的数据流)。主机 B

向主机 A 发送 SYN 报文段的目的是实现从主机 B 到主机 A 的序列号的同步，即确定 seq 中的 Y。主机 B 向主机 A 发送确认信息 ack＝X＋1，这是因为在 TCP 连接过程中，把正确接收到的最后一个序列号再加 1 的和，作为现在的确认号。

（3）主机 A 发送 ACK 给主机 B：我的确认序号 ack 是 Y＋1。

通过以上三个步骤（三次握手），TCP 连接建立，开始传输数据。

2. 数据传输

在连接建立后，TCP 将以全双工方式传送数据，在同一时间主机 A 与主机 B 之间可以同时进行 TCP 报文段的传输，并对接收到的 TCP 报文段进行确认。如图 5-19 所示，当通过三次握手建立了主机 A 与主机 B 之间的 TCP 连接后，现在假设主机 A 要向主机 B 发送 1800 字节的数据，主机 B 要向主机 A 发送 1500 字节的数据。

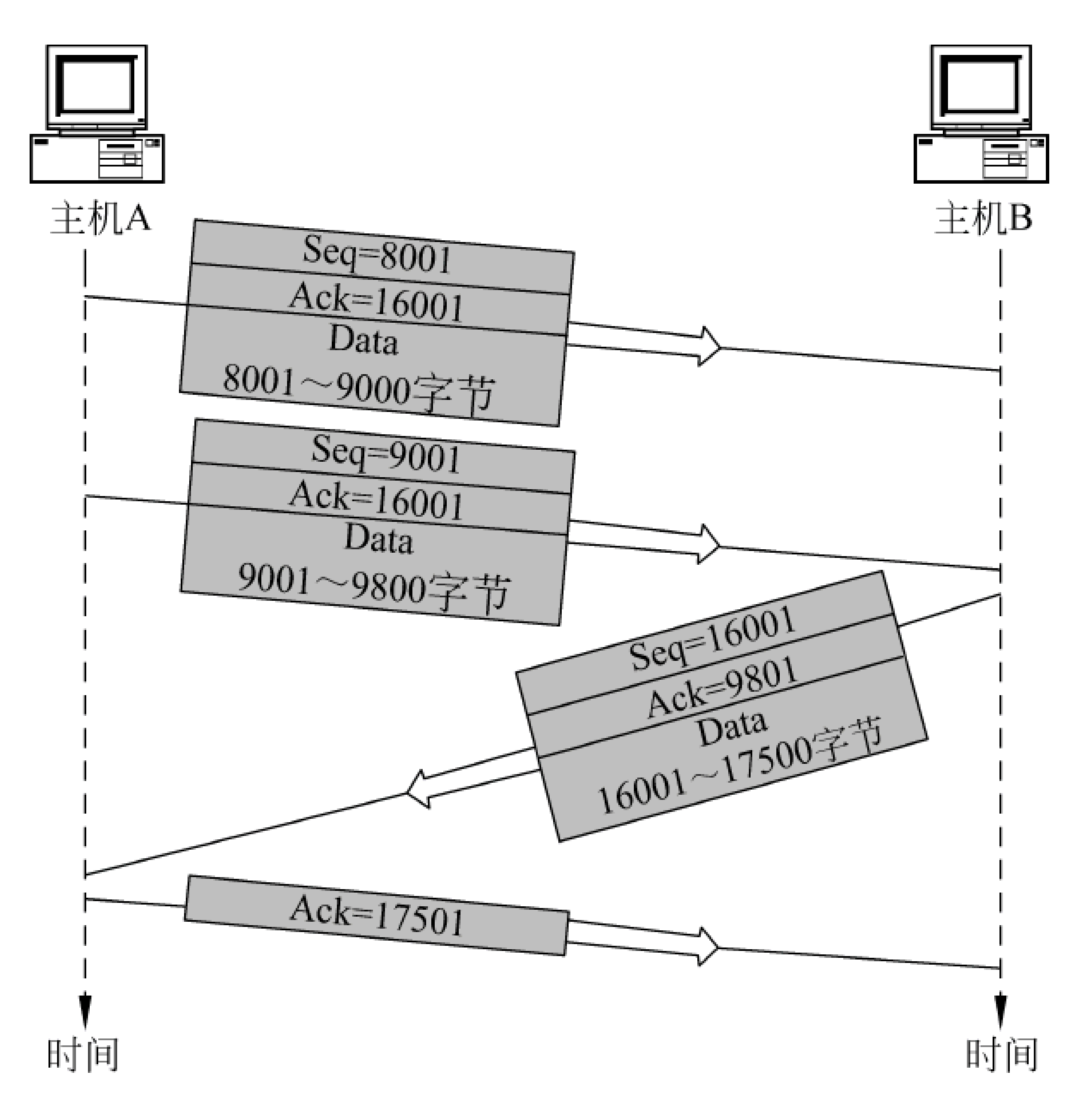


图 5-19　TCP 报文段的传输过程

在 TCP 报文段的首部信息中有一个序号字段和一个确认序号字段，在数据传输过程中要用到这两个字段的功能特性。TCP 把一个连接中发送的所有数据都要按字节进行编号，而且在两个方向上的编号是互不影响的。当主机要发送数据时，TCP 从应用进程中接收数据，并将其存储在发送缓存中，然后按字节进行编号，这也是为什么将 TCP 报文称为字节流的原因。编号并不一定从 0 开始，而是在 0～($2^{32}-1$)之间取一个随机数作为第一个字节的编号。例如，在本例中主机 A 正好取了 8001 作为第一个字节的编号，由于数据总长度为 1800，所以字节的编号从 8001～9801。同理，主机 B 的字节编号假设为 16001～17500。

当对字节进行了编号后，TCP 就给每一个报文段分配一个序号，该序号即这个报文段中的第一个字节的编号。在本例中，主机 A 发送的数据被分成两个报文段（每 1000 字节为一段），由于第一个字节的编号为 8001，所以第一个报文段的序号 seq＝8001。第二个报文段只有 800 字节，第二个报文段中的第一个字节的编号为 9001，所以第二个报文段的序号 seq＝9001。主机 B 正好以 1500 字节为一个报文段，所以主机 B 发送给主机 A 的数据正好存放在一个报文段中，该报文段的序号 seq＝16001。

每一个报文段可以选择不同的路径在网络中进行传输，在接收端需要对接收到的报文段进行确认。前文已经提到，在 TCP 中确认序号被定义为下一个希望接收到的字节的编号，所以在本例中当主机 B 成功接收到主机 A 发送过来的第二个报文段时，由于该报文段中的字节编号为 9001～9800，所以主机 B 发送给主机 A 的确认序号 ack＝9801。

另外，在本例中还有三个问题需要进行说明。一是确认信息由发送信息同时捎带。每一个报文段中的 ack 序号就是对已成功接收到的报文段的确认；二是为了提高 TCP 的传输效率，主机并不会对接收到的每一个报文段报送确认信息，而是当同时接收到多个报文段后再发送确认信息，所以在本例中主机 B 只对主机 A 发送了一个确认信息；三是主机 A 在最后一次只发送了一个 Ack＝17501 的确认信息，表示已成功接收到了主机 B 发送过来的报文段。这是因为主机 A 在本次 TCP 连接中已经没有数据再进行发送。

3. 连接终止

对于一个已经建立的连接，TCP 使用改进的三次握手来释放连接(使用一个带有 FIN 附加标记的报文段，即在 TCP 报文段首部中将 FIN 字段的值置为 1)。TCP 关闭连接的步骤如图 5-20 所示。

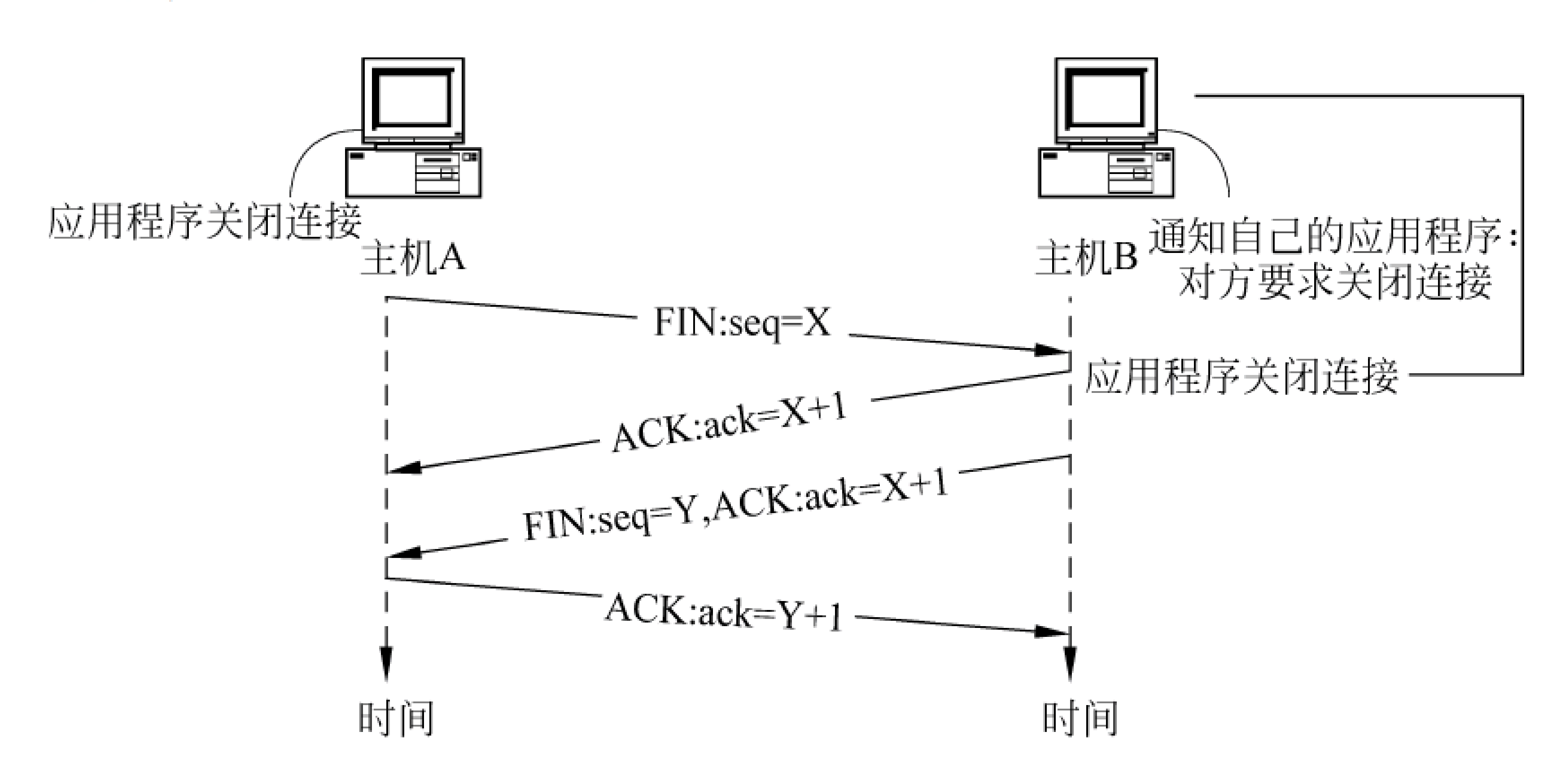


图 5-20　TCP 使用改进的三次握手来释放连接

(1) 当主机 A 的应用程序通知 TCP 数据已经发送完毕时，TCP 向主机 B 发送一个带有 FIN 附加标记的报文段(FIN 表示英文 finish)。

(2) 主机 B 收到这个 FIN 报文段之后，并不立即用 FIN 报文段回复主机 A，而是先向主机 A 发送一个确认序号 ACK，同时通知自己相应的应用程序：对方要求关闭连接(先发送 ACK 的目的是为了防止在这段时间内，对方重传 FIN 报文段)。

(3) 主机 B 的应用程序告诉 TCP：我要彻底的关闭连接，TCP 向主机 A 发送一个 FIN 报文段。

(4) 主机 A 收到这个 FIN 报文段后，向主机 B 发送一个 ACK 报文段，表示连接彻底释放。

5.4.2　TCP 的安全问题

在 TCP/IP 网络中，如果两台主机之间要实现可靠的数据传输，首先要通过三次握手方式建立主机之间的 TCP 连接。但在 TCP 连接过程中很容易出现一个严重的安全问题：TCP SYN 泛洪攻击。

按照 TCP 连接建立时三次握手的协议约定，当源主机 A 要建立与目的主机 B 之间的 TCP 连接时，源主机 A 首先发送一个用于同步的 SYN 报文段(第一次握手)。当目的主机 B 接收到这个报文段时，在正常情况下目的主机会打开连接端口，并给源主机 A 返回一个 SYN+ACK 的报文段(第二次握手)。同时，目的主机 B 将这个处于“半开放状态”的连接放在等待队列中，等待源主机 A 的 ACK 确认报文段(即等待第三次握手的实现)。这段等待时间一般为 75s～25min。

TCP SYN 泛洪攻击的工作过程如图 5-21 所示。如果在每一次握手过程中，源主机 A 发送给目的主机 B 的 SYN 报文段中的 IP 地址是伪造的，同时源主机 A 同时向目的主机 B 发送大量的 SYN 报文段。这时，对于目的主机 B 来说会正常接收这些 SYN 报文段，并发送 SYN+ACK 确认报文段。由于目的主机 B 接收到的 SYN 报文段中的 IP 地址都是伪造的，所以发送出去的 SYN+ACK 确认报文段全部得不到回复。在目的主机 B 的队列中存在大量的“半开放状态”的连接，最终将队列的存储空间填满，并因资源耗尽而瘫痪。

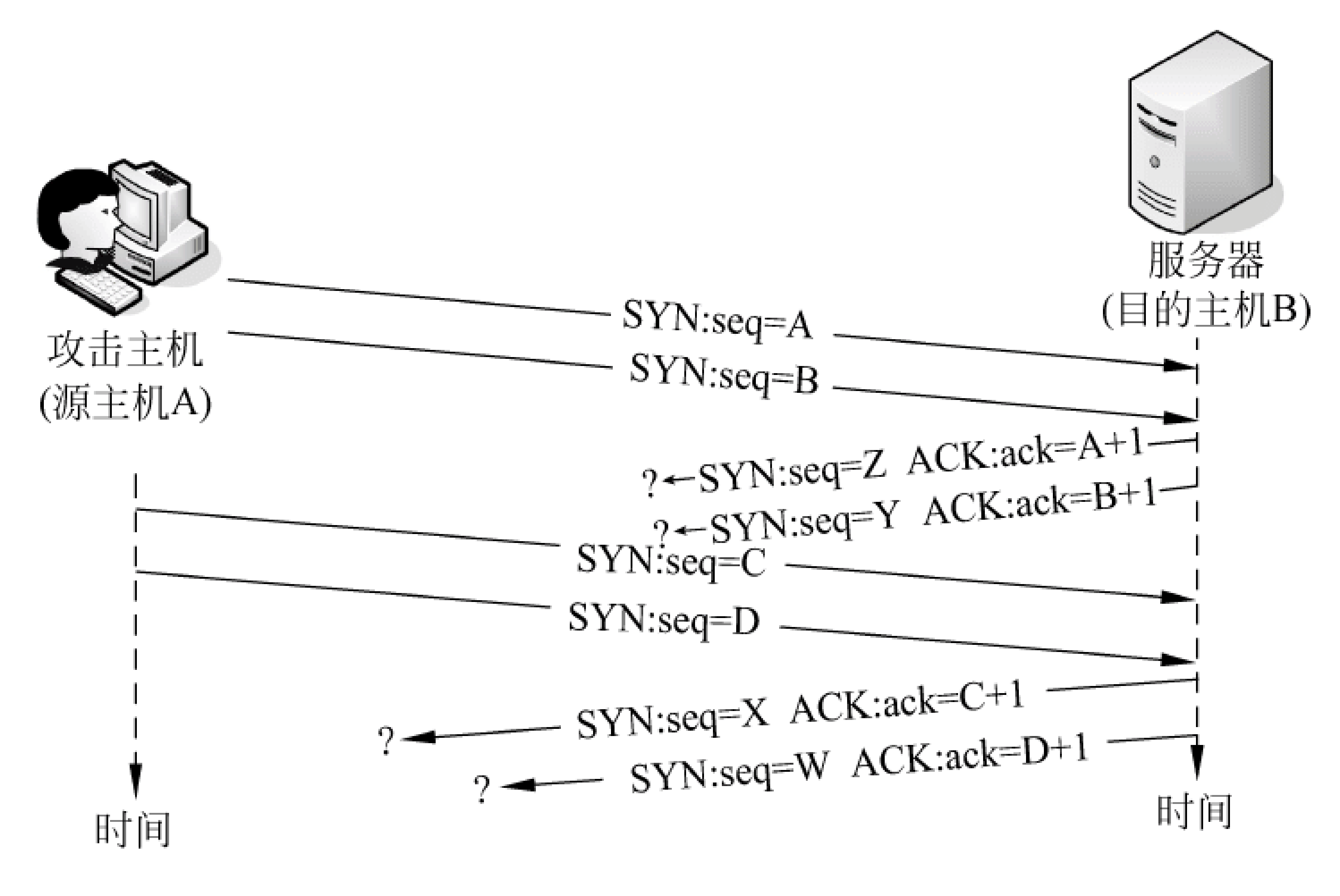


图 5-21　TCP SYN 泛洪攻击的工作过程

这种 TCP SYN 泛洪攻击属于一种典型的拒绝服务攻击(DoS 攻击)，即攻击者使用大量的服务请求耗尽了服务器的资源，使服务器无法处理正常的服务请求，最终造成系统的瘫痪。

5.4.3　实验操作 3　操作系统中 TCP SYN 泛洪的防范

可以在 Windows 注册表内配置 TCP/IP 参数，以便保护服务器免遭网络级别的 TCP SYN 泛洪攻击。下面以 Windows 2000/2003 为例进行介绍。

1. 启用 TCP SYN 攻击保护

启用 TCP SYN 泛洪攻击保护的命名值，位于注册表项：HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services 的下面。

值名称：SynAttackProtect

建议值：2

有效值：0～2

说明：使 TCP 调整 SYN+ACK 的重传。配置此值后，在遇到 TCP SYN 攻击时，对连

接超时的响应将更快速。在超过 TcpMaxHalfOpen 或 TcpMaxHalfOpenRetried 的值后，将触发 SYN 攻击保护。

2. 设置 TCP SYN 保护阈值

下列值确定触发 SYN 保护的阈值。这一部分中的所有注册表项和值都位于注册表项 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services 下。这些注册表项和值如下。

值名称：TcpMaxPortsExhausted

建议的数值数据：5

有效值：0～65535

说明：指定触发 TCP SYN 泛洪攻击保护所必须超过的 TCP 连接请求数的阈值。

值名称：TcpMaxHalfOpen

建议的数值数据：500

有效值：100～65535

说明：在启用 SynAttackProtect 后，该值指定处于 SYN_RCVD 状态的 TCP 连接数的阈值。在超过 SynAttackProtect 后，将触发 TCP SYN 泛洪攻击保护。

值名称：TcpMaxHalfOpenRetried

建议的数值数据：400

有效值：80～65535

说明：在启用 SynAttackProtect 后，该值指定处于至少已发送一次重传的 SYN_RCVD 状态中的 TCP 连接数的阈值。在超过 SynAttackProtect 后，将触发 TCP SYN 泛洪攻击保护。

3. 设置其他保护

这一部分中的所有注册表项和值都位于注册表项 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services 下。这些注册表项和值如下。

值名称：TcpMaxConnectResponseRetransmissions

建议的数值数据：2

有效值：0～255

说明：控制在响应一次 SYN 请求之后、在取消重传尝试之前 SYN+ACK 的重传次数。

值名称：TcpMaxDataRetransmissions

建议的数值数据：2

有效值：0～65535

说明：指定在终止连接之前 TCP 重传一个数据段(不是连接请求段)的次数。

值名称：EnablePMTUDiscovery

建议的数值数据：0

有效值：0,1

说明：将该值设置为 1(默认值)可强制 TCP 查找在通向远程主机的路径上的最大传输单元或最大数据包大小。攻击者可能将数据包强制分段，这会使堆栈不堪重负。对于不是来自本地子网的主机的连接，将该值指定为 0 可将最大传输单元强制设为 576 字节。

值名称：KeepAliveTime

建议的数值数据：300000

有效值：80～4294967295

说明：指定 TCP 尝试通过发送持续存活的数据包，来验证空闲连接是否仍然未被触动的频率。

值名称：NoNameReleaseOnDemand

建议的数值数据：1

有效值：0，1

说明：指定计算机在收到名称发布请求时是否发布其 NetBIOS 名称。

使用表 5-1 中汇总的值可获得最大程度的保护。

表 5-1　建议值

值名称	值(REG_DWORD)
SynAttackProtect	2
TcpMaxPortsExhausted	1
TcpMaxHalfOpen	500
TcpMaxHalfOpenRetried	400
TcpMaxConnectResponseRetransmissions	2
TcpMaxDataRetransmissions	2
EnablePMTUDiscovery	0
KeepAliveTime	300000(5 分钟)
NoNameReleaseOnDemand	1

5.4.4　实验操作 4　TCP 端口的查看与限制

本实验的内容对于一些专用服务器非常有效。例如，对于 Web 服务器，可以只开放 TCP 80 端口；对于 FTP 服务器，可以只开放 TCP 21 端口等。常见端口的使用情况如表 5-2 所示。

表 5-2　常用端口号的使用情况

常用的应用层协议或应用程序	端　口　号	
	UDP	TCP
FTP		21
TELNET		23
SMTP		25
DNS	53	
TFTP	69	
SNMP	161	
HTTP		80
DHCP		67
RPC(远程过程调用)		135

1. Windows 操作系统已开放端口的查看方法

Windows 操作系统提供了 netstat 命令来显示当前 TCP/IP 网络的连接情况。具体方法如下所示(以 Windows Server 2003 为例)。

选择“开始”→“程序”→“附件”→“命令提示符”,进入“命令提示符”窗口。输入命令 netstat-na,按 Enter 键后将显示如图 5-22 所示的信息。

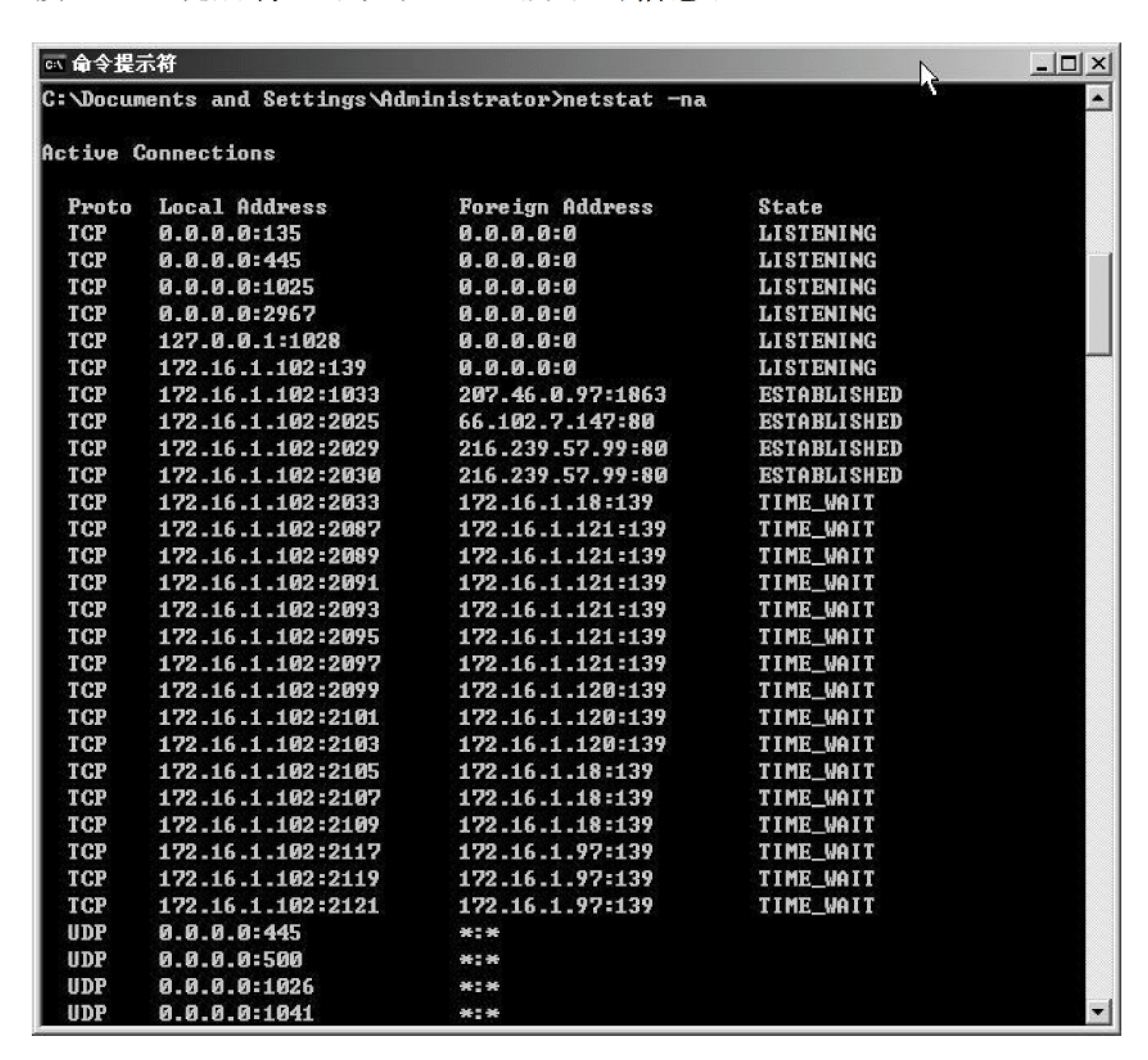


图 5-22　利用 netstat-na 命令显示当前打开的端口

- Active Connections。是指当前本机的活动连接。
- Proto。是指连接使用的协议名称,为 TCP 或 UDP。
- Local Address。下面显示了本机 IP 地址和打开的端口号,如 172.16.1.102:139,其中 172.16.1.102 为本机的 IP 地址,139 为打开的一个 TCP 端口。
- Foreign Address。是连接该端口的远程计算机的 IP 地址和端口号。
- State。表明当前 TCP 的连接状态。其中,LISTENING 是监听状态,表明本机正在对打开的端口进行监听,等待远程计算机的连接;ESTABLISHED 表示已建立的连接,说明两台主机之间正在通过 TCP 协议进行通信;TIME_WAIT 的意思是结束了这次连接,说明该端口曾经有过访问,但访问结束了。需要注意的是,UDP 端口不需要进行监听。

通过以上分析,凡是 State 显示为 LISTENING 的端口都是比较危险的,有可能会被病毒或黑客所利用,作为入侵系统的端口。

如果在 DOS 窗口中输入了 netstat-nab 命令,还将显示每个连接都是由哪些程序创建的,如图 5-23 所示。

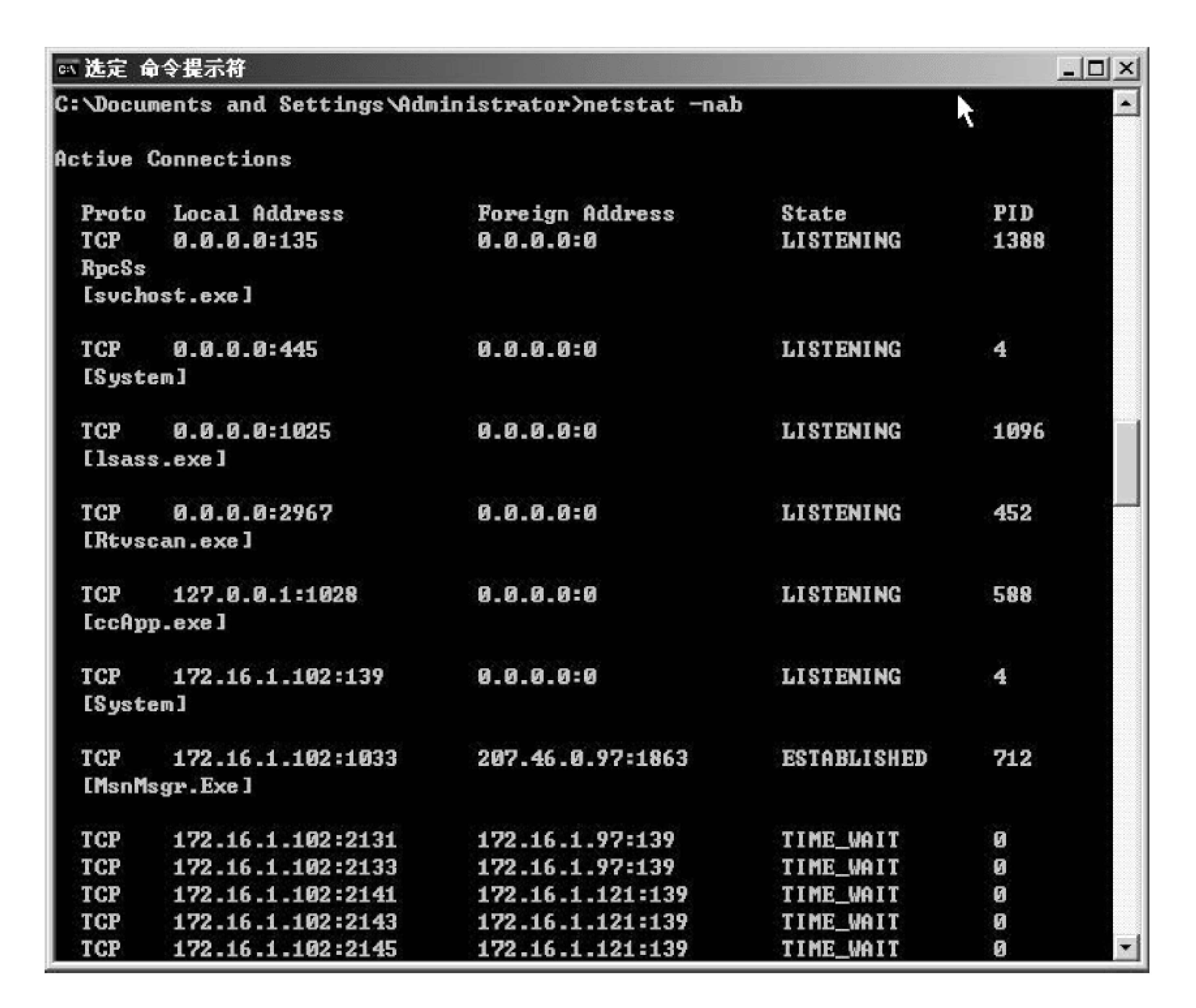


图 5-23 利用 netstat-nab 命令显示哪些应用程序在使用当前打开的端口

从图 5-23 可以看出，本机的 135 端口监听就是由 svchost. exe 程序创建的。利用该命令，如果用户发现本机打开了可疑的端口，就可以查看它调用了哪些应用程序，然后再检查各应用程序的创建时间和修改时间，如果发现异常，就可能是中了木马病毒。

另外，也可以使用一些专门的端口监视软件来查看本机打开了哪些端口。这类软件非常多，如 Tcpview、Port Reporter、绿鹰 PC 万能精灵和网络端口查看器等。图 5-24 所示的是 Tcpview 的操作界面，该软件会密切监视本机端口连接情况，这样就能严防非法连接，确保网络安全。

该软件不但可以方便地查看端口号，而且还能够查看到当前该端口对应的应用程序。例如，一些单位不允许职工在上班期间使用 QQ，这时网络管理员便可以利用 Tcpview 软件来查出当前 QQ 使用的 UDP 端口范围，然后在网络出口处将其封掉。

2. 限制 TCP 端口

端口是应用层程序（进程）与传输层协议（TCP 或 UDP）之间的连接通道。通过端口限制功能，可以只允许计算机通过指定的 TCP 或 UDP 端口来通信，其他端口的通信功能将被全部关闭。下面假设在一台 Web 服务器上只开放 TCP 80 端口，只允许用户使用系统默认的 TCP 80 端口访问服务器上的 HTTP 页面，而无法从事其他的网络访问，以加强对专用 Web 服务器的安全保护。以 Windows Server 2003 为例，具体设置如下。

（1）在服务器上打开网卡的“本地连接属性”对话框，选取“Internet 协议（TCP/IP）”选项，单击“属性”按钮。

（2）在打开的对话框中单击“高级”按钮，并在出现的对话框中选择“选项”选项卡，打开如图 5-25 所示的“高级 TCP/IP 设置”对话框。

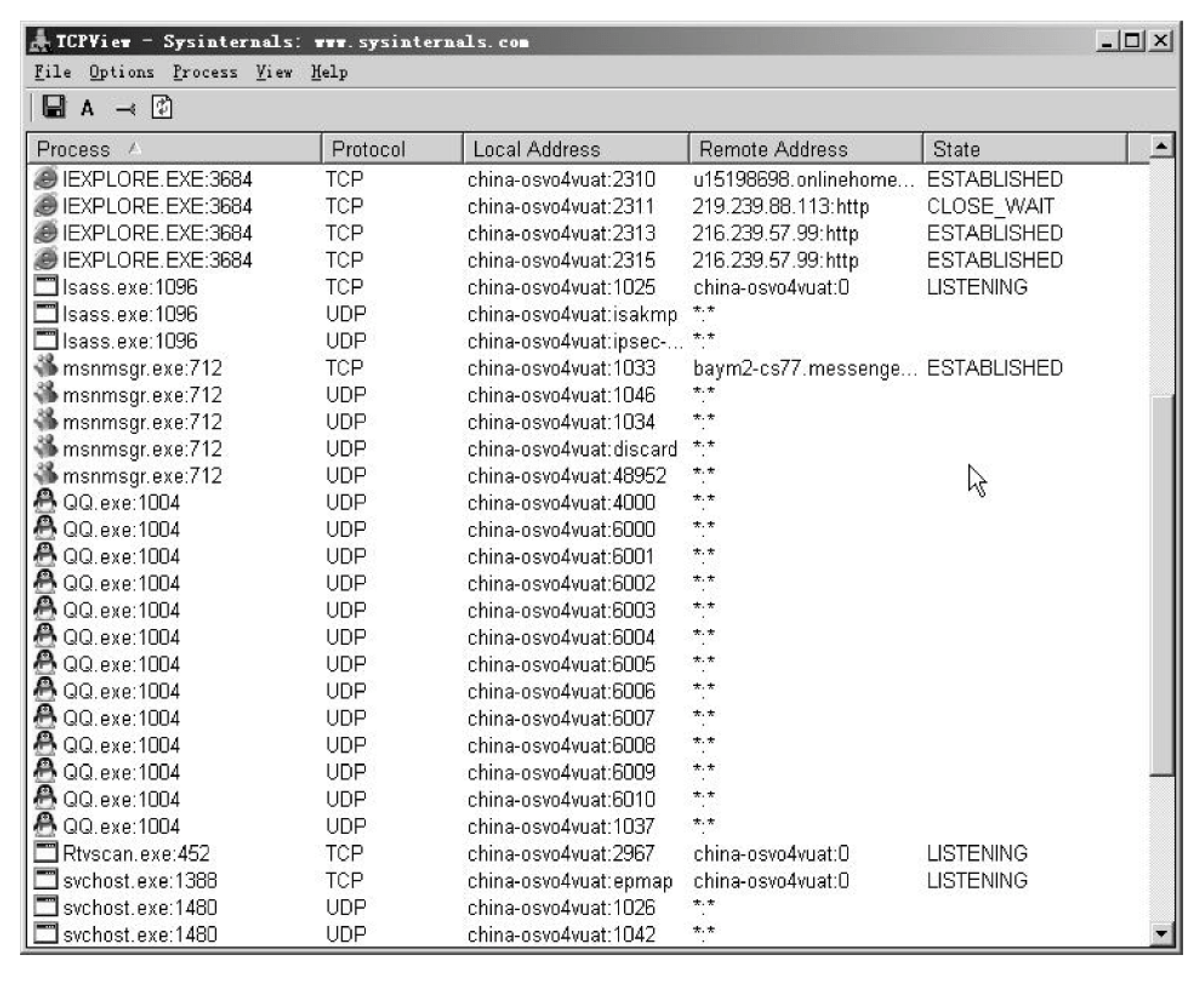


图 5-24　Tcpview 软件的操作界面

（3）单击“属性”按钮，在打开的如图 5-26 所示的“TCP/IP 筛选”对话框中选取“启用 TCP/IP 筛选(所有适配器)”复选框，同时选取“TCP 端口”栏中的“只允许”单选按钮，并单击“添加”按钮，在出现的对话框中将“TCP 端口”设置为 80。

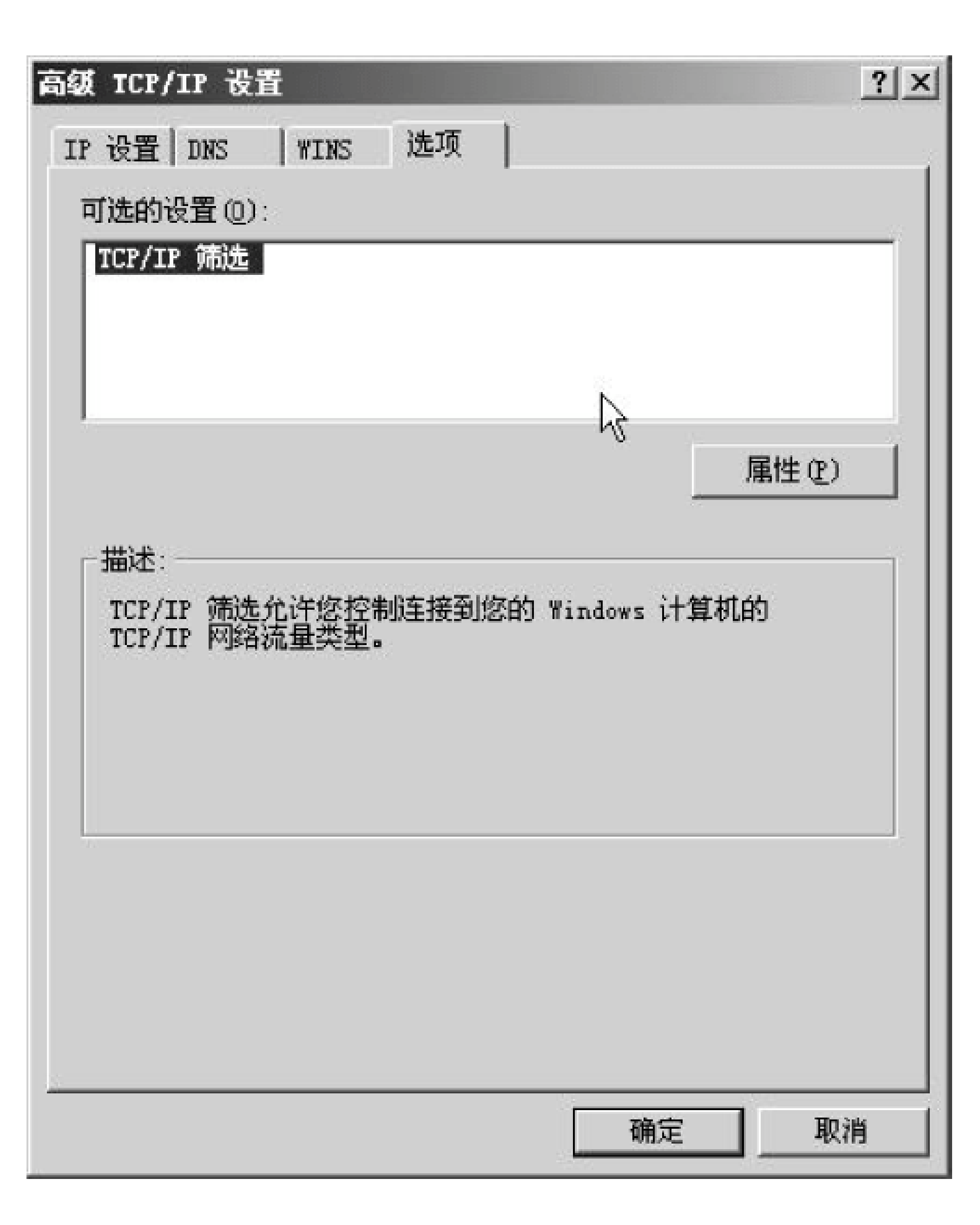


图 5-25　“高级 TCP/IP 设置”对话框中的“选项”选项卡



图 5-26　设置 TCP 或 UDP 端口

（4）单击"确定"按钮，进行确认。

读者可以根据以上设置，再结合实际应用，通过配置 TCP 或 UDP 端口来对专业服务器进行安全保护。

3. 限制 IP 地址的访问

通过限制主机的 TCP 或 UDP 的端口，可以对一些专业服务器进行安全保护。如果一台服务器上提供了 Web、FTP 和 Mail 等多项服务，同一项服务（如 Web）还可能同时存在多个站点，且不同站点采取不同的安全保护策略。这时可以利用 IP 地址限制功能实现对某一项应用的安全管理。不管是 TCP 报文段，还是 UDP 数据报，在网际层后都要封装到 IP 分组中进行传输，所以对 IP 地址的限制可同时适用于 TCP 和 UDP。

下面以 Windows Server 2003 操作系统为例，设置 IIS 中的"默认网站"只能由 IP 地址在 172.16.0.0/16 网段中的主机来访问，当使用其他 IP 地址的主机访问时被拒绝（读者也可以在 IIS 中先发布一个网站，再对发布的网站进行配置）。具体设置方法如下（必须已安装了"Internet 信息服务（IIS）"）。

（1）选择"开始"→"程序"→"管理工具"→"Internet 信息服务"，打开"Internet 信息服务（IIS）管理器"窗口。

（2）选取"网站"下的"默认网站"，单击鼠标右键，在弹出的快捷菜单中选择"属性"命令，在打开的"默认网站属性"对话框中选择"目录安全性"选项卡，打开如图 5-27 所示的对话框。

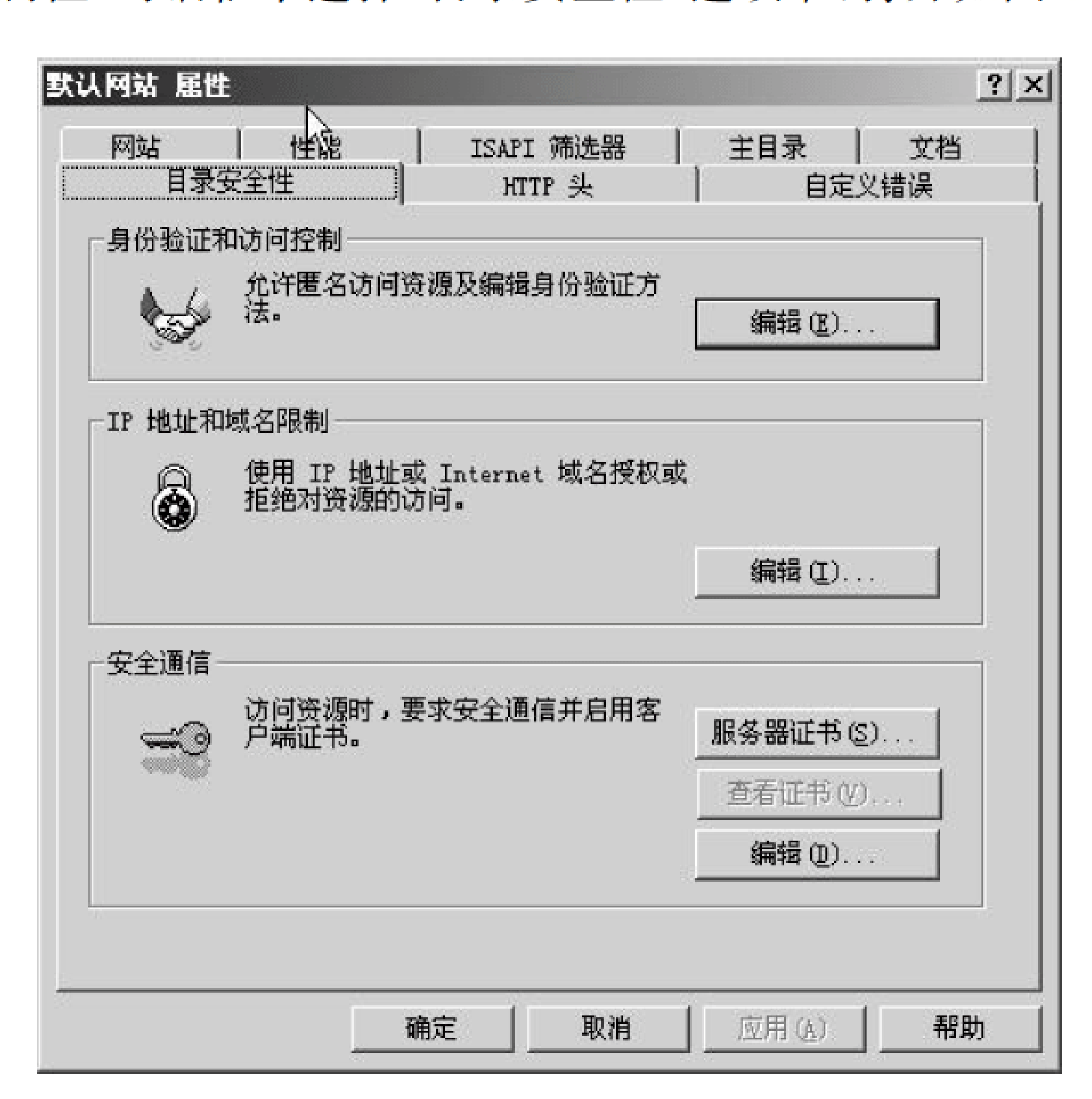


图 5-27 "默认网站属性"对话框中的"目录安全性"选项卡

（3）单击"IP 地址和域名限制"选项区域中的"编辑"按钮，打开如图 5-28 所示的"IP 地址和域名限制"对话框。系统默认设置为"授权访问"，即允许所有主机的访问。

（4）选择"拒绝访问"单选按钮，然后单击"添加"按钮，在打开的如图 5-29 所示的"授权访问"对话框中选取"一组计算机"单选按钮，并在"网络标识"文本框中输入允许访问该网站的计算机所在的网段 IP（本例为 172.16.0.0），在"子网掩码"文本框中输入该网段的子网掩码（本例为 255.255.0.0）。



图 5-28　系统默认不进行 IP 地址限制



图 5-29　输入允许访问的网段 IP 及子网掩码

(5) 单击“确定”按钮，172.16.0.0/16 地址段将添加到允许访问列表框中，如图 5-30 所示。

(6) 单击“确定”按钮，完成设置。



图 5-30　显示已设置的 IP 地址段

这时，在一台能够访问该 Web 服务器，但 IP 地址不在 172.16.0.0/16 范围内的计算机上输入 http://172.16.2.10(其中 172.16.2.10 为 Web 服务器的 IP 地址)，将会显示如图 5-31 所示的提示信息，说明该计算机不具备访问该 Web 网站的权限。

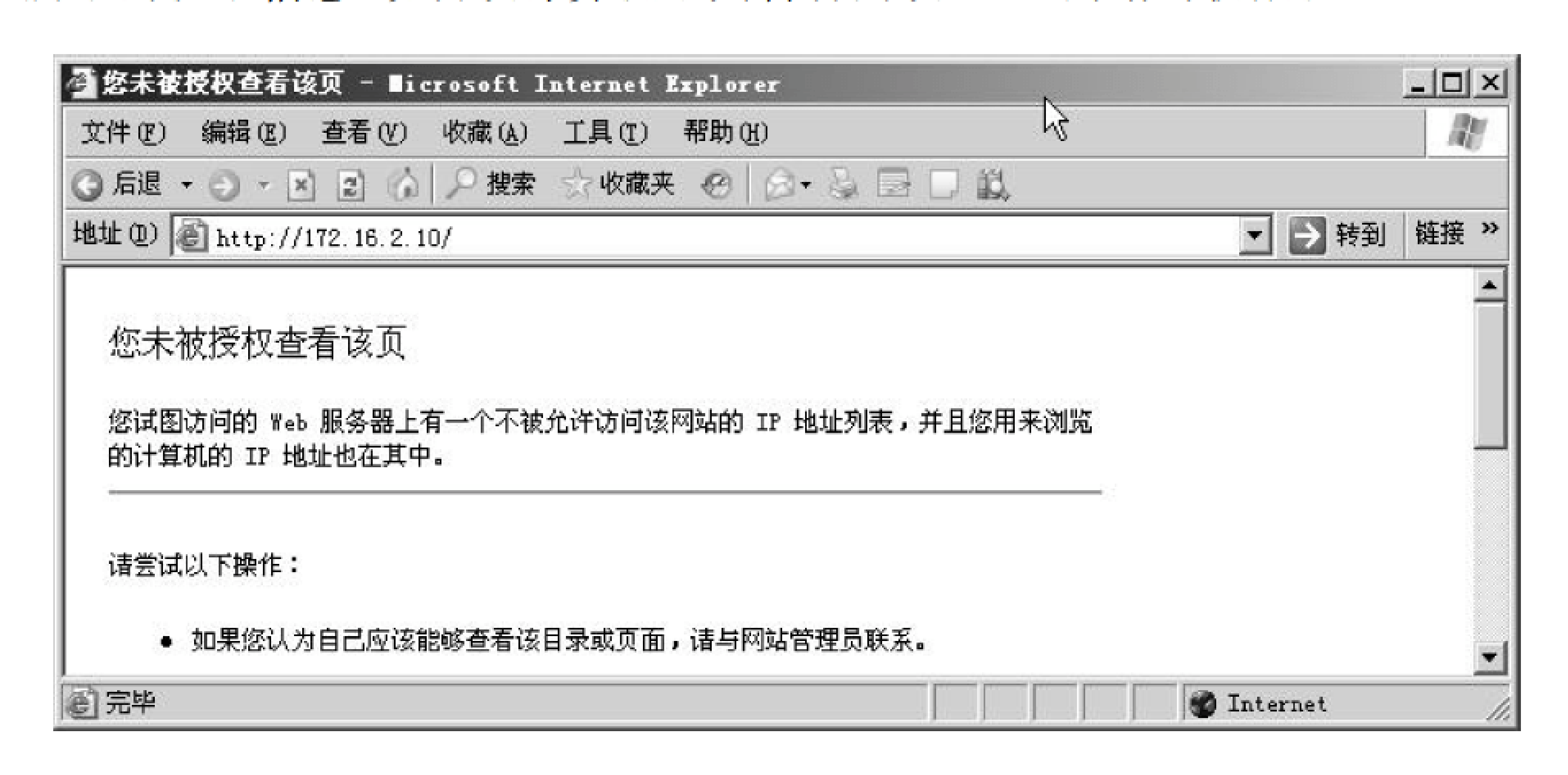


图 5-31　拒绝用户访问该 Web 网站时的提示信息

5.5 DNS 安 全

为了解决主机 IP 地址与主机名之间的对应关系，InterNIC（Internet Network Information Center，Internet 网络信息中心）制定了一套称为域名系统（Domain Name System，DNS）的分层名字解析方案。当 DNS 用户提出 IP 地址查询请求时，就可以由 DNS 服务器中的数据库提供所需的数据。DNS 技术目前已广泛地应用于 Internet 和 Intranet 中。

5.5.1 DNS 概述

DNS 是一组协议和服务，它允许用户在查找网络资源时使用层次化的对用户友好的名字取代 IP 地址。当 DNS 客户端向 DNS 服务器发出 IP 地址的查询请求时，DNS 服务器可以从其数据库内寻找所需要的 IP 地址给 DNS 客户端。这种由 DNS 服务器在其数据库中找出客户端 IP 地址的过程叫做“主机名称解析”。

1. DNS 的功能及组成

简单地讲，DNS 协议最基本的功能是对主机名与对应的 IP 地址之间建立映射关系。例如，新浪网站的一个 IP 地址是 202.106.184.200，几乎所有浏览该网站的用户都是使用 www.sina.com.cn，而并非使用 IP 地址来访问。使用主机名（域名）比直接使用 IP 地址具有以下两点好处。

（1）主机名便于记忆，如 sina.com.cn。

（2）数字形式的 IP 地址可能会由于各种原因而改变，而主机名可以保持不变。

DNS 的工作任务是在计算机主机名与 IP 地址之间进行映射。DNS 位于 TCP 参考模型的最高层，使用 TCP 和 UDP 作为传输协议（一般多使用 UDP，因为 UDP 的系统开销较小）。DNS 模型相当简单：客户端向 DNS 服务器提出访问请求（如 www.sina.com.cn），DNS 服务器在收到客户端的请求后在数据库中查找相对的 IP 地址（202.106.184.200），并作出反应。如果该 DNS 服务器无法提供对应的 IP 地址（如数据库中没有该客户端主机名对应的 IP 地址）时，它就转给下一个它认为更好的 DNS 服务器去处理。

当需要给某人打电话时，你可能知道这个人的姓名，而不知道他的电话号码。这时，可以通过查看电话号码簿查得他的电话号码，从而与他进行通话。由此可以看出，电话号码簿的功能便是建立姓名与电话号码之间的映射关系。而 DNS 的功能与这里的电话号码簿很类似。

DNS 是为 TCP/IP 网络提供的一套协议和服务，是由名字分布数据库组成的。它建立了叫做域名空间的逻辑树结构，是负责分配、改写、查询域名的综合性服务系统。该空间中的每个节点或域都有一个唯一的名字。

组成 DNS 系统的核心是 DNS 服务器，它是回答域名服务查询的计算机，允许为私人 TCP/IP 网络和连接公共 Internet 的用户提供并管理 DNS 服务，维护 DNS 名字数据并处理 DNS 客户端主机名的查询。DNS 服务器保存了包含主机名和相应 IP 地址的数据库。例如，如果提供了名字 www.sina.com，DNS 服务器将返回新浪网站的 IP 地址 202.106.184.200。

DNS 是一种看起来与磁盘文件系统的目录结构类似的命名方案，域名也通过使用句点“.”分隔每个分支来标识一个域在逻辑 DNS 层次中相对于其父域的位置。但是，当定位一个文件位置时，是从根目录到子目录再到文件名，如 C:\winnt\win.exe；而当定位一个主机名时，是从最终位置到父域再到根域，如 sina.com。

图 5-32 显示了顶级域的名字空间及下一级子域之间的树型结构关系，图中的每一个节点及其下的所有节点叫做一个域。域可以有主机(计算机)和其他域(子域)。例如，在图 5-32 中，pc1.sd.cninfo.net 就是一台主机，而 sd.cninfo.net 则是一个子域。一般在子域中含有多台主机，例如，ah.cninfo.net 子域下就含有 pc1.ah.cninfo.net 和 pc30.ah.cninfo.net 两台主机。

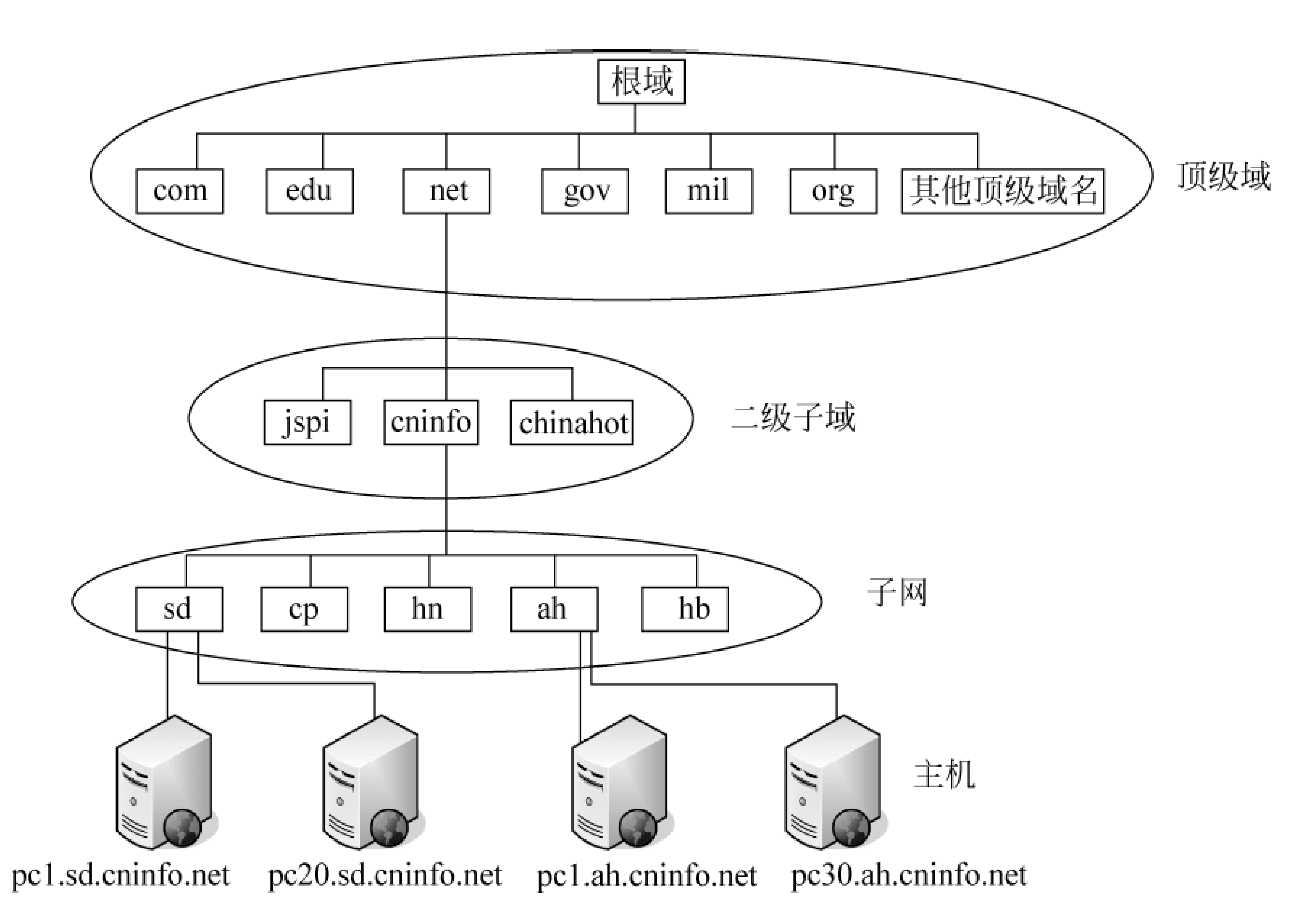


图 5-32　Internet 的域名结构

- 根域。代表域名命名空间的根，这里为空。
- 顶级域。直接处于根域下面的域，代表一种类型的组织和一些国家。在 Internet 中，由 InterNIC 进行管理和维护。如在顶级域名中 com 代表商业组织、edu 代表教育和学术机构等，在域名的国家代码中 cn 代表中国、us 代表美国等。
- 二级域。在顶级域下面，用来标明顶级域以内的一个特定的组织。在 Internet 中，也是由 InterNIC 负责对二级域名进行管理和维护，以保证二级域名的唯一性。
- 子域。在二级域的下面所创建的域，一般由各个组织根据自己的要求自行创建和维护。
- 主机。是域名命名空间中的最下面一层，它被称之为完全合格的域名(Fully Qualified Domain Name，FQDN)。

2. DNS 的解析过程

现在假设客户端 Web 浏览器要访问网站 www.sina.com，整个访问过程如图 5-33 所示。具体描述如下：

(1) Web 浏览器调用 DNS 客户端程序(该程序称为“解析器”)，先在本地的 DNS 缓存

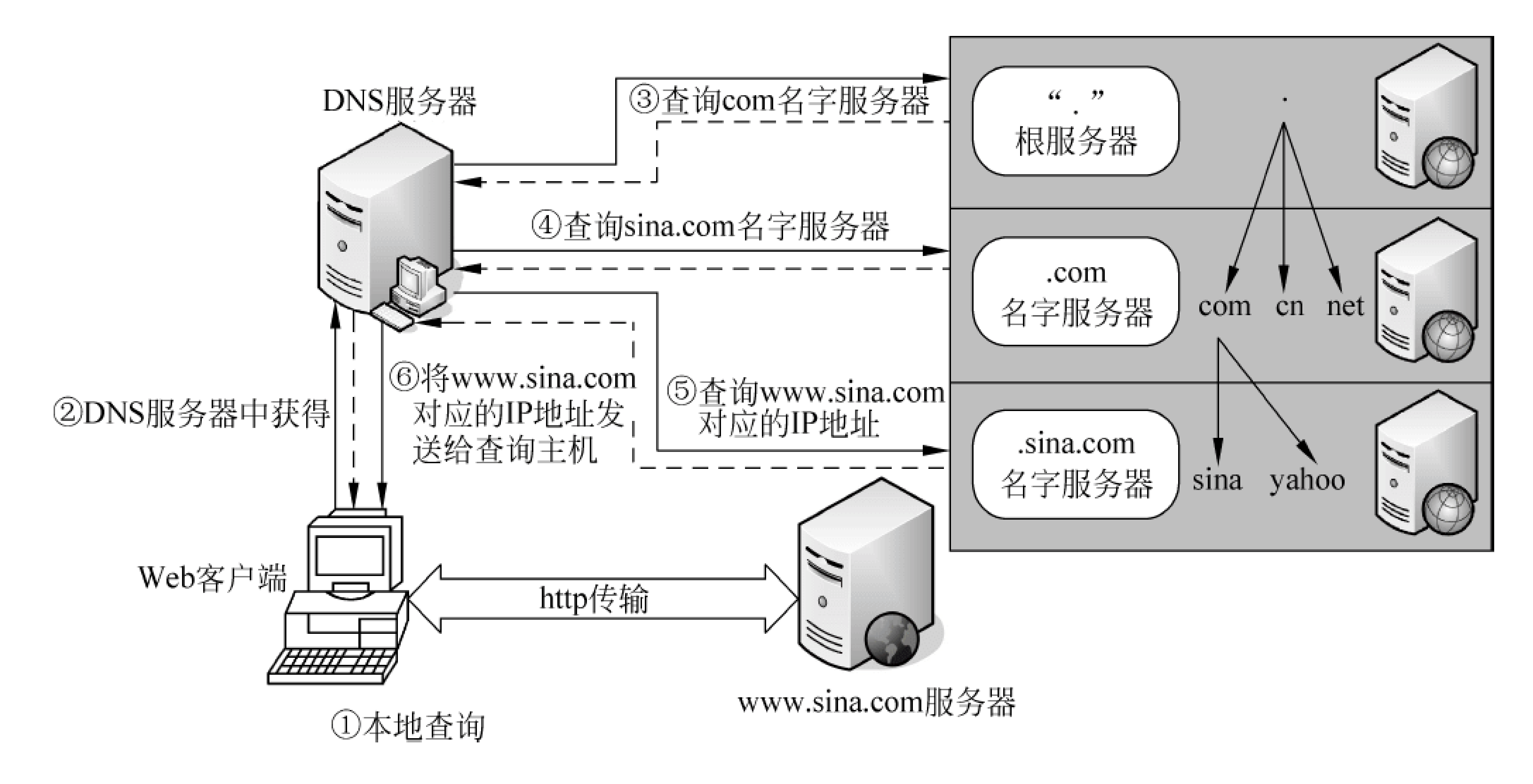


图 5-33　Internet 上对 www. sina. com 的访问过程

中查询是否有 www. sina. com 的记录。如果有该记录（例如，Web 浏览器刚刚访问过 www. sina. com，缓存中的记录系统还没有删除），则直接访问。

（2）如果在本地的缓存中没有找到相关的记录，客户端就会根据已设置的 DNS 服务器记录，向 DNS 服务器发出查询请求。如果该 DNS 服务器正好是创建 www. sina. com 记录的服务器，或在特定的时间段内处理过相同的查询，那么它就会从自己的区域记录或缓存中检索到该域名相应的资源记录（Resource Record，RR），并返回给客户端。

（3）否则 DNS 服务器就将查询转发给根域服务器，由根域服务器找到 com 名字服务器地址，并发送给 DNS 服务器。

（4）DNS 服务器向 com 名字服务器继续发出查询 www. sina. com 地址的请求，com 名字服务器在找到 sina. com 的地址后，将结果发送给 DNS 服务器。

（5）DNS 服务器向 sina. com 名字服务器发出查询 www. sina. com 的请求，sina. com 名字服务器检索到 www. sina. com 对应的 IP 地址，并将结果发送给 DNS 服务器。

（6）DNS 服务器将 www. sina. com 对应的资源记录发送给 Web 客户端，Web 客户端利用 IP 地址访问相应的主机。

同时，在以上的递归查询过程中，Web 客户端、DNS 服务器及各级的名字服务器都会记录这一次查询结果，以便下一次查询时直接调用。

5.5.2　DNS 的安全问题

DNS 服务是一种最基础的网络服务，但是 DNS 在设计之初并没有考虑安全问题，只是为了方便人们使用，简单地在域名与 IP 地址之间进行了映射，并将映射记录提供给人们查询，DNS 内部没有为数据提供任何安全认证和数据完整性检查，留下了极大的安全隐患。如果 DNS 服务器被入侵者控制，则有可能篡改 DNS 服务器数据中 IP 地址与主机名之间的映射关系，从而会使主机遭受各类攻击（如 DoS 攻击、Web 欺骗攻击等），严重时有可能造成单位内部网络（Intranet）或 Internet 中名称解析的混乱。下面介绍几种常见的 DNS 安全威胁。

1. 缓存中毒

DNS为了提高查询效率，采用了缓存机制，把用户查询过的最新记录存放在缓存中，并设置生存周期(Time To Live，TTL)。在记录没有超过TTL之前，DNS缓存中的记录一旦被客户端查询，DNS服务器(包括各级名字服务器)将把缓存区中的记录直接返回给客户端，而不需要进行逐级查询，提高了查询速率。

DNS缓存中毒利用了DNS缓存机制，在DNS服务器的缓存中存入大量错误的数据记录主动供用户查询。由于缓存中大量错误的记录是攻击者伪造的，而伪造者可能会根据不同的意图伪造不同的记录，例如将查询指向某一个特定的服务器，使所有通过该DNS查询的用户都访问某一个网站的主页；或将所有的邮件指向某一台邮件服务器，拦截利用该DNS进行解析的邮件等。

由于DNS服务器之间会进行记录的同步复制，所以在TTL内，缓存中毒的DNS服务器有可能将错误的记录发送给其他的DNS服务器，导致更多的DNS服务器中毒。正如DNS的发明者Paul Mockapetris所说：中毒的缓存就像是"使人们走错方向的假冒路牌"。

2005年8月，数十万台因特网上的DNS服务器遭受到DNS缓存中毒的攻击，攻击者将存储在DNS服务器上的流行网站的IP地址更换为恶意网站的IP地址，将毫不知情的因特网用户由合法的网站引导到恶意网站，并要求用户透露机密信息或安装恶意软件。

DNS数据库对因特网上的用户是完全开放的，它既没有在DNS内部对数据提供认证机制和完整性检查，也没有对DNS服务器提供的服务进行访问控制和限制。所以攻击者可以将一些未经验证的数据存入到DNS服务器的缓存中，同时当用户在DNS服务器上进行地址查询时，DNS服务器也不对用户进行任何身份认证。DNS的这种工作机制造成了大量的安全漏洞，使DNS遭受到了各种各样的安全攻击。

2. 拒绝服务攻击

DNS服务器在因特网中的关键作用使它很容易成为攻击者进行攻击的目标，加上DNS服务器对大量的攻击没有相应的防御能力，所以攻击过程很容易实现，且造成的后果非常严重。现在使用的DNS采用了树形结构，一旦DNS服务器不能提供服务，其所辖的子域都将无法解析客户端的域名查询请求。

对DNS服务器进行拒绝服务攻击比较容易。目前针对DNS服务器的拒绝服务攻击主要有两种方式：一种是直接攻击DNS服务器，将DNS服务器作为被攻击对象，由多台攻击主机向被攻击的DNS服务器频繁发送大量的DNS查询请求，最终使DNS服务器崩溃；另一种是利用DNS服务器作为"中间人"，去攻击网络中的其他主机。攻击者可以向多个DNS服务器发送大量的查询请求，这些查询请求数据包中的源IP地址为被攻击者的IP地址。DNS服务器将大量的查询结果发送给被攻击主机，使被攻击主机无法提供正常的服务，例如使DNS服务器无法为用户提供正常的查询等。

3. 域名劫持

域名劫持通常是指通过采用非法手段获得某一个域名管理员的账户和密码，或者域名管理邮箱，然后将该域名的IP地址指向其他的主机(该主机的IP地址有可能不存在)。域名被劫持后，不仅有关该域名的记录会被改变，甚至该域名的所有权可能会落到其他人的手里。

2001年3月25日，"我要"(51.com)电子商务网站遭到攻击，其域名删除达一天之久。

这是我国第一例涉嫌域名劫持的事件。就其事件的整个过程来说，就是攻击者首先通过电子邮件获得了 51.com 网站的域名管理员账户和密码，然后删除正常的域名解析记录。

5.5.3 DNS 安全扩展

为了弥补 DNS 最初设计时存在的安全缺陷，1994 年 IETF 成立了 DNSSEC(DNS Security)工作组，通过在原有协议上增添 DNSSEC 部分，从而从整体上解决 DNS 的安全问题。1999 年 3 月，IETF 以 RFC 2535 文档发布了 DNSSEC(Domain Name System Security Extensions，域名系统安全扩展)，提出了解决 DNS 安全问题的一系列措施。

1. DNSSEC 的基本原理

域名系统安全扩展是在原有的域名系统上通过公钥技术，对 DNS 中的信息进行数字签名，从而提供 DNS 的安全认证和信息完整性检验。具体原理如下。

发送方：首先使用 Hash 函数对要发送的 DNS 信息进行计算，得到固定长度的"信息摘要"；然后对"信息摘要"用私钥进行加密，此过程实现了对"信息摘要"的数字签名；最后将要发送的 DNS 信息、该 DNS 信息的"信息摘要"及该"信息摘要"的数字签名一起发送出来。

接收方：首先采用公钥系统中的对应公钥对接收到的"信息摘要"的数字签名进行解密，得到解密后的"信息摘要"；接着用与发送方相同的 Hash 函数对接收到的 DNS 信息进行运算，得到运算后的"信息摘要"；最后对解密后的 "信息摘要"和运算后的"信息摘要"进行比较，如果两者的值相同，就可以确认接收到的 DNS 信息是完整的，即是由正确的 DNS 服务器得到的响应。

由此可以看出，在 DNSSEC 中所有返回给域名解析器(DNS 客户端程序)的响应都附加了数字签名。域名解析器通过数字签名来验证这些记录与权威的域名服务器上的记录是否完全一致。数字签名采用的是公钥加密系统，它产生的密钥对分为公钥和私钥两部分。其中，私钥需要保密存储，用来对区域文件中的 DNS 信息的"数字摘要"进行加密；公钥需要在 DNS 服务器上公开发布，域名解析器接收到域名服务器发送的响应记录后，使用公钥对响应记录中的数字签名进行解密，将得到的值与所接收到的 DNS 信息进行 Hash 运算获得的值进行对比，如果相同，说明该记录是合法的。

为了实现上述功能，DNSSEC 定义了三种资源记录(RR)：用于存放 DNS 信息数字签名的 SIG RR、用于存放解密公钥的 KEY RR 和用于存放否定应答(即不存在资源记录)的 NXT RR。

2. DNSSEC 的工作机制

在 DNS 系统中，每一个 DNS 服务器可以管理一个区域，例如 com.cn 就是一个区域(zone)，在该区域上再创建子区域(称为"子域")，如 sina.com.cn、yahoo.com.cn 等。

DNSSEC 对 DNS 区域中的记录进行签名和验证是建立在对该区域信任的基础上。为了实现对区域密钥的信任，需要由父域对子域进行验证。DNS 系统为一树形结构，DNS 客户端通过递归方式进行域名的查询，在一个完整的 DNS 递归查询过程中，第一个要查询的名字服务器为根域服务器(如图 5-33 所示)。在 DNSSEC 系统中，DNS 客户端的域名解析器首先确保根域是可信任的，然后信任由根域签名的子域，并依此类推。

这种从根域开始，由上到下逐级签名验证的方式被称为信任链(Trusted Chain)，即父

域与子域之间逐级建立信任关系。由此可以看出，根域是整个 DNSSEC 的安全入口，每一个支持 DNSSEC 的 DNS 客户端解析器都需要建立与根域之间的信任关系，即需要安装根域的公钥。同时，根域以下的 DNS 服务器之间也要通过公钥系统建立信任关系。一般情况下，每一个区域通过相应的密码算法产生一个公钥/私钥对，并保存在该区域的一个权威名字服务器内。在域名查询过程中，当查询到某一个区域时，由该区域的权威名字服务器用自己的私钥对 DNS 信息的“摘要信息”进行数字签名，该区域（父域）的下级区域（子域）用公钥对签名数据进行解密。

图 5-34 所示的是一个 DNSSEC 系统的查询和应答过程。其中，系统中的所有客户端和服务器都支持 DNSSEC，区域 abc. cn 的权威名字服务器为 auth. abc. cn，区域 xyz. net 的权威名字服务器为 auth. xyz. net。

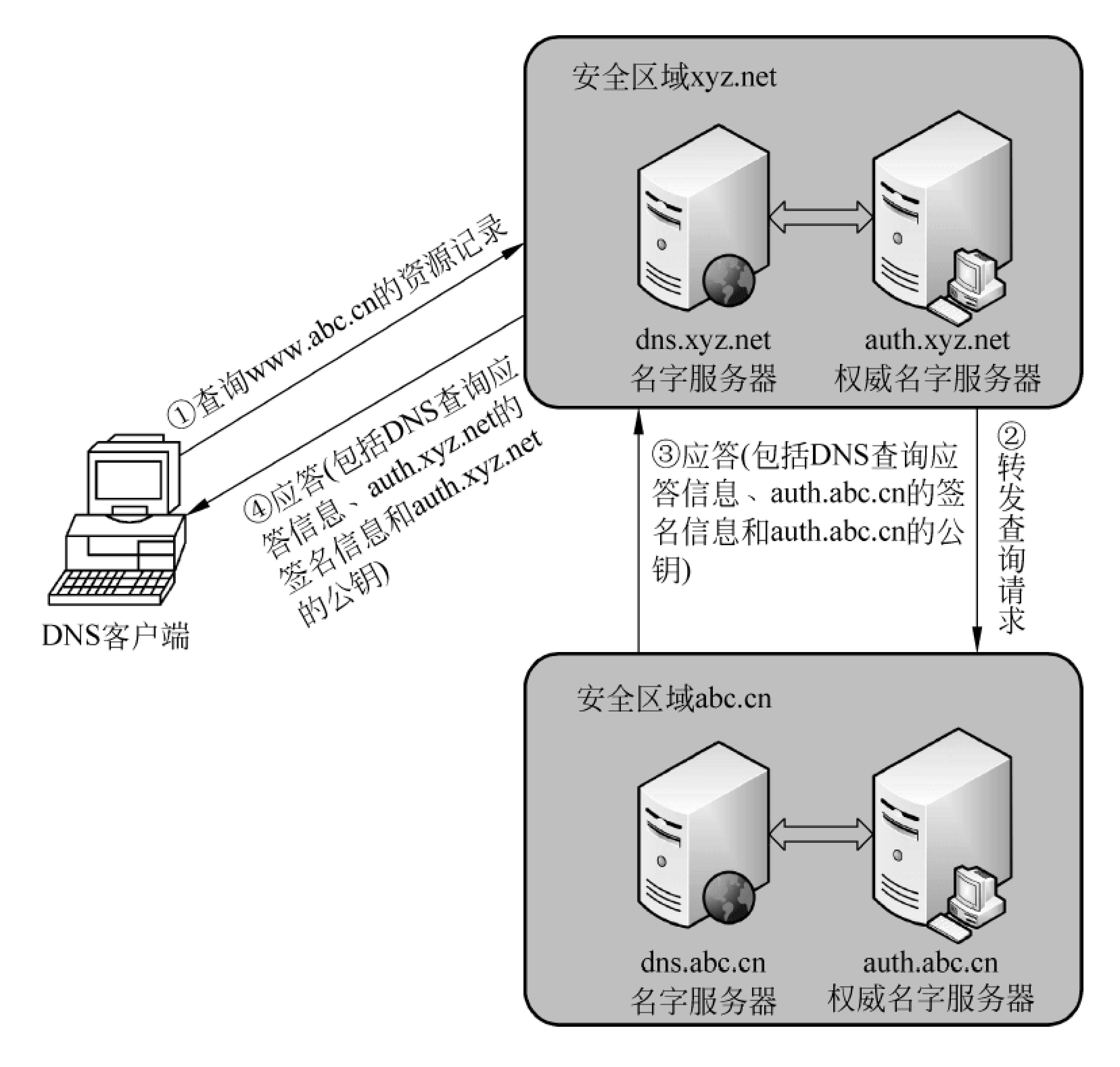


图 5-34　DNSSEC 系统的查询和应答过程

现在，客户端要查询 www. abc. cn。具体查询过程为：由于 DNS 客户端设置的 DNS 服务器的地址指向了 dns. xyz. net，所以 DNS 客户端向名字服务器 dns. xyz. net 发送一个查询请求，请求 www. abc. cn 的资源记录。假设 dns. xyz. net 服务器的缓存中没有该记录，dns. xyz. net 服务器便将该查询请求发给 dns. abc. cn 服务器，最后由 dns. abc. cn 服务器查询到了 www. abc. cn 的资源记录。因为安全区域 abc. cn 授权 auth. abc. cn 服务器管理本区域中的密钥，而安全区域 xyz. net 授权 auth. xyz. net 服务器管理本区域中的密钥，所以 auth. abc. cn 服务器将 www. abc. cn 查询的应答信息用自己的私钥进行签名并转发给 auth. xyz. net 服务器，auth. xyz. net 服务器对接收到的签名信息用 auth. abc. cn 服务器的公钥进行解密，以验证应答信息的安全性和完整性。当 auth. xyz. net 服务器通过验证后，再将应答信息转发给 DNS 客户端，此过程也要利用数字签名验证应答信息的安全性和完整性。

3. DNSSEC 的应用现状

DNSSEC 作为对目前 DNS 的安全扩展，可有效地防范 DNS 存在的各种攻击，保证客户端收到的 DNS 记录的真实性和完整性。此外，DNSSEC 与原有的 DNS 具有向下的兼容性，在实现上具有可行性。但是，由于 Internet 的特殊性，就像从 IPv4 到 IPv6 的迁移一样，从 DNS 到 DNSSEC 的转换不可能在短期内完成，需要一个渐进的过程。可以先有针对性地建立一些安全区域，如 . cn、. net 等，然后再向其他区域扩展。当整个 Internet 部署了 DNSSEC 后，所有的信任将集中到根域下。

在 DNSSEC 系统中，不但 DNS 服务器要支持安全扩展功能，而且 DNS 客户端也要支持该功能。目前，基于 Windows Server 2003、Linux 和 UNIX 等操作系统的 DNS 服务器都可以支持 DNSSEC，Windows XP/Vista、Linux 等较新操作系统的 DNS 客户端也已支持 DNSSEC。

但是，目前在推广 DNSSEC 上存在许多问题或困难：一是由于整个 Internet 上的 DNS 记录非常庞大，如果要部署适用于整个 Internet 的 DNSSEC，需要投入大量时间和设备，同时还要得到所有区域服务器提供商的支持。二是 DNSSEC 只是提供了对 DNS 记录真实性的验证，只是在有限的程度上为用户通信的安全提供了保证。但要完全保证用户信息的安全，还需要对应用程序和数据传输的各个环节加强其安全性。三是 DNSSEC 在 DNS 请求和应答中添加了数字签名，一方面增加了通信的流量和复杂性，另一方面安全性主要依赖于公钥技术的安全性，所以对于 DNSSEC 系统来说是否会存在新的安全问题也是一个未知数。

5.5.4 实验操作 5 DNS 系统的安全设置

DNS 系统的安全涉及到 DNS 服务器、DNS 客户端、路由器和防火墙等设备或系统，下面仅介绍一些常用的安全技术和措施。

1. 选择安全性较高的 DNS 服务器软件

Internet 上大量的 DNS 服务器软件使用的是基于 UNIX/Linux 的 BIND 软件，目前最新版本为 BIND 9. x。最新版本的 BIND 软件支持许多安全特性，如支持 DNSSEC，解决了早期版本中存在的一些安全漏洞等。对于在 Internet 上的 DNS 服务器建议采用 BIND 软件，并将其升级为最新版本。

随着 Windows NT 系统的广泛使用，许多中小企业使用 Windows NT 自带的 DNS 软件组建 DNS 服务器。对于这些用户，一方面建议使用 Windows Server 2003 作为服务器操作系统，利用 Windows Server 2003 操作系统自身的安全性增加 DNS 服务器的安全性；另一方面是在一台 Windows Server 2003 的域控制器上创建 DNS 服务器，这样可以利用活动目录的安全功能加强对 DNS 的安全管理。如果用户的 DNS 服务器建立在没有域的独立服务器上，建议将其升级为一台域控制器。

2. 限制端口

DNS 在工作时使用 UDP 53 和 TCP 53 端口进行通信。其中，DNS 服务器会同时监听这两个端口，DNS 客户端通过 UDP 53 端口与 DNS 服务器之间进行域名解析的请求和应答，而 TCP 53 端口用于 DNS 区域之间的数据复制。

为此，对于专用 DNS 服务器，可通过防火墙的设置或直接在 DNS 服务器操作系统上的

设置,只开放 UDP 53 和 TCP 53 两个端口,限制其他端口的通信,通过端口限制功能来加强系统的安全性。Windows 操作系统中的操作方法可参阅本章 5.4.4 节中"限制 TCP 端口"的内容。

根据教学需要,本章结合 TCP/IP 参考模型重点介绍了 ARP、DHCP、TCP 和 DNS 协议的工作原理及存在的安全问题,并结合实际应用提出了一些可行的解决方法。其实,本章的内容仅是对 TCP/IP 参考模型中安全问题的一个初探,从目前的应用和研究来看,TCP/IP 中的每一个协议几乎都存在安全问题。为此,希望读者通过本章的学习,通过参阅相关资料,加深对通信协议的理解和分析,在以后的工作中提高网络的安全性。

习 题

5-1 联系 OSI 参考模型,介绍 TCP/IP 参考模型的分层特点及各层的功能。

5-2 结合图 5-4,描述互联网络中两台主机之间的通信过程。

5-3 结合 ARP 协议的工作特点,描述 ARP 欺骗的工作原理。

5-4 结合 TCP/IP 网络中计算机和交换机的工作原理,分别描述针对计算机和交换机的 ARP 欺骗的特点。

5-5 在中小网络中如何防范 ARP 欺骗?并通过实验进行验证。

5-6 结合 DHCP 的工作原理和网络运行实际,指出目前计算机网络中针对 DHCP 存在的主要安全问题及产生的危害。

5-7 如何通过对交换机和操作系统的设置加强 DHCP 服务的安全?

5-8 在掌握 TCP 传输三个过程的基础上,分析 TCP 协议存在的安全问题,并结合实际提出相应的解决方法。

5-9 结合 DNS 的工作过程,描述 DNS 缓存中毒、拒绝服务攻击和域名劫持的实现过程。

5-10 描述 DNSSEC 的工作原理和工作过程。

第6章 计算机病毒、木马和间谍软件与防治

近年来，随着计算机网络的广泛应用，全球信息化不断加快，以计算机网络为平台的信息技术和应用已触及社会生活的各个角落。但由于计算机网络所固有的结构松散、系统开放、主机和终端具有多样性等特点，致使网络易受病毒、黑客、恶意软件和其他不良行为的破坏或影响。我们应该对计算机网络进行全方位的安全防范，以保障网络系统的正常运行，其中计算机病毒的防治是最为普遍和有效的一种安全措施。本章将从计算机病毒的特征、危害和发展等基本知识入手，在对计算机病毒、木马和间谍软件有一个总体认识后，将有针对性地介绍一些病毒的特征及防治方法。

6.1 计算机病毒概述

从单机操作开始，计算机病毒的危害性已被大多数人所共知。在计算机网络广泛使用的今天，计算机病毒几乎遍及到每一台计算机，只是所造成的危害不同而已。就像每一个人会不同程度的存在一些不健康因素一样，每一台计算机都存在着病毒的侵害。

6.1.1 计算机病毒的概念

计算机病毒(virus)的传统定义是指人为编制或在计算机程序中插入的，破坏计算机功能或者毁坏数据、影响计算机使用，并能自我复制的一组计算机指令或者程序代码。现在计算机病毒的定义已远远超出了以上的定义，其中破坏的对象不仅仅是计算机，同时还包括交换机、路由器等网络设备；影响的不仅仅是计算机的使用，同时还包括网络的运行性能。就像许多生物病毒具有传染性一样，绝大多数计算机病毒具有独特的复制能力和感染良性程序的特性。

借助计算机网络，计算机病毒可以快速地蔓延，一旦某一病毒发作将很难进行控制和根除。计算机病毒将其自身附着在各种类型的文件(如可执行文件、图片文件和电子邮件等)上，当附有计算机病毒的文件被复制或从一台主机传送到另一台主机时，它们就随同文件一起蔓延开来。目前，计算机病毒已成为网络安全的主要威胁之一。

种类繁多的计算机病毒将导致计算机或网络系统瘫痪，程序和数据严重破坏；使网络产生阻塞，运行效率大大降低；使计算机或网络系统的一些功能无法正常使用；使电子银行、电子政务等网上信息交换存在欺骗性等诸多影响。层出不穷的各种各样的计算机病毒活跃在网络的每个角落，如近几年的冲击波、震荡波、灰鸽子、QQ尾巴、网游盗号木马和熊猫烧香病毒等，给用户的正常工作造成了严重威胁。

6.1.2 计算机病毒的特征

计算机或网络病毒本身也是一个或一段计算机程序，只是该程序是用来破坏计算机系统或影响计算机系统正常运行的“恶性”程序。从计算机病毒的本质来看，它具有以下几个明显特征。

1. 非授权可执行性

用户通常在调用并执行一个程序时，系统会将控制权交给这个程序，并分配给该程序相应的系统资源（如内存等），从而使之能够运行完成用户的需求。因此程序执行的过程对用户是透明的。而计算机病毒是非法程序，不过正常用户是不会知道该程序是病毒程序，从而像调用正常的程序一样来调用并执行。但由于计算机病毒具有正常程序的一切特性：可存储性和可执行性，当计算机病毒隐藏在合法的程序或数据中，在用户运行正常程序时，病毒便会伺机窃取到系统的控制权，并得以抢先运行。然而，此时用户还认为在执行正常程序。

2. 隐蔽性

计算机病毒是一种由编程人员编写的短小精悍的可执行程序。它通常附着在正常程序或磁盘的引导扇区中，同时也会存储在表面上看似损坏的磁盘扇区中，因此计算机病毒具有非法可存储性。计算机病毒不管是在存在方式还是传播途径上都会想方设法地隐藏自己，以尽量避开用户或查病毒软件。

3. 传染性

传染性是计算机病毒最重要的特征，也是各类查病毒软件判断一段程序代码是否为计算机病毒的一个重要依据。病毒程序一旦侵入计算机系统就开始搜索可以传染的程序或者磁介质，然后通过自我复制迅速进行传播。由于目前计算机网络的应用非常广泛，这就使计算机病毒可以在极短的时间内传播到其他的计算机上，尤其是 Internet 的应用更为计算机病毒的传播提供了全球性的高速通道。

4. 潜伏性

计算机病毒具有依附于其他程序的能力，所以计算机病毒具有寄生能力。将用于寄生计算机病毒的程序（良性程序）称之为计算机病毒的宿主。依靠病毒的寄生能力，计算机病毒在传染良性程序后，有时不会马上发作，而在隐藏一段时间后在一定的条件（如时间，例如“黑色星期五病毒”）下开始发作。这样，病毒的潜伏性越隐蔽，它在系统中存在的时间也就越长，病毒传染的范围也越广，其危害性也就越大。

5. 破坏性

无论是何种病毒程序，一旦侵入计算机系统都会对操作系统的运行造成不同程度的影响。即使不直接产生破坏作用的病毒程序也要占用系统的资源（如内存空间、磁盘存储空间等）。而绝大多数病毒程序在运行时要显示一些文字或图像，会影响系统的正常运行。还有一些病毒程序会删除系统中的文件，或加密磁盘中的数据，甚至摧毁整个系统，使系统无法恢复，造成无法挽回的损失。因此，病毒程序轻则降低系统的运行效率，重则导致系统崩溃或数据丢失。计算机病毒的破坏性表现了绝大多数计算机病毒设计者的真正意图。

6. 可触发性

计算机病毒一般都有一个或者几个触发条件，当满足该触发条件后计算机病毒便会开始发作。触发的实质是一种条件的控制，病毒程序可以依据设计者的要求，在一定条件下实

施攻击。这个条件可以是输入的特定字符、特定文件、特定日期或特定时刻,也可以利用病毒内置的计数器来实现触发。

6.1.3 计算机病毒的分类

一些病毒被设计为通过损坏程序、删除文件或重新格式化硬盘来损坏计算机。有些病毒不损坏计算机,而只是复制自身,并通过显示文本、视频和音频消息表明它们的存在。即使是这些良性病毒也会给计算机用户带来影响。通常它们会占用合法程序使用的计算机内存,使正常的程序运行产生异常,甚至导致系统崩溃。另外,许多病毒包含大量错误,这些错误可能导致系统崩溃和数据丢失。根据 Symantec 等公司的总结,目前可识别的计算机病毒可以分为以下 5 类。

1. 文件传染源病毒

文件传染源病毒感染程序文件。这些病毒通常感染可执行代码,例如.com 和.exe 文件等。当受感染的程序从软盘、U 盘或硬盘上运行时,可以感染其他文件。这些病毒中有许多是内存驻留型病毒。内存受到感染之后,运行的任何未感染的可执行文件都会受到感染。已知的文件传染源病毒包括 Jerusalem、Cascade 等。

2. 引导扇区病毒

引导扇区病毒感染磁盘的系统区域,即软盘、U 盘和硬盘的引导记录。所有软盘、U 盘和硬盘(包括仅包含有数据的磁盘)的引导记录中都包含一个小程序,该程序在计算机启动时运行。引导扇区病毒将自身附加到磁盘的这一部分,并在用户试图从受感染的磁盘启动时激活。这些病毒本质上通常都是内存驻留型病毒。其中大部分引导扇区病毒是针对 DOS 编写的,但所有计算机(无论使用什么操作系统)都是此类病毒的潜在目标。只要试图用受感染的软盘或 U 盘启动计算机就会被感染。此后,由于病毒存在于内存中,因此访问软盘或 U 盘时,所有未写保护的软盘或 U 盘都会受到感染。引导扇区病毒主要包括 Form、Disk Killer、Michelangelo 和 Stoned 等。

3. 主引导记录病毒

主引导记录病毒是内存驻留型病毒,它感染磁盘的方式与引导扇区病毒相同。这两种病毒类型的区别在于病毒代码的位置。主引导记录感染源通常将主引导记录的合法副本保存在另一个位置,受到引导扇区病毒或主引导扇区病毒感染的 Windows NT/2000/2003 计算机将不能启动,这是由于 Windows NT/2000/2003 操作系统访问其引导信息的方式与 Windows 9x 不同。早期,如果 Windows NT 使用 FAT 分区格式化,通常可以通过启动到 DOS 系统,并使用防病毒软件来清除病毒。如果引导分区是 NTFS,则必须使用三张 Windows NT 安装盘才能恢复系统。不过,现在的 DOS 启动可以同时支持 FAT 和 NTFS 两种方式。主引导记录病毒主要有 NYB、AntiExe 和 Unashamed 等。

4. 复合型病毒

复合型病毒同时感染引导记录和程序文件,并且被感染的记录和程序较难修复。如果清除了引导区,但未清除文件,则引导区将再次被感染。同样,只清除受感染的文件也不能完全清除该病毒。如果未清除引导区的病毒,则清除过的文件将被再次感染。复合型病毒包括 One_Half、Emperor、Anthrax 和 Tequilla 等。

5. 宏病毒

宏病毒是目前最常见的病毒类型，它主要感染数据文件。随着 Microsoft Office 97 中 Visual Basic 的出现，编写的宏病毒不仅可以感染数据文件，还可以感染其他文件。宏病毒可以感染 Microsoft Office Word、Excel、PowerPoint 和 Access 文件。现在，这类新威胁也出现在其他程序中。所有这些病毒都使用其他程序的内部程序设计语言，创建该语言的原意是使用户能够在该程序内部自动执行某些任务。这些病毒很容易创建，现在传播着的就有几千种，曾经广泛流行的宏病毒主要包括 W97M. Melissa、Macro. Melissa（美丽莎）、WM. NiceDay 和 W97M. Groov 等。

6.1.4 病毒、蠕虫和木马

病毒、蠕虫和木马是破坏计算机和计算机中信息的恶意程序。但病毒、蠕虫和木马之间在本质上还是有区别的。

1. 病毒的特点

计算机病毒是编写的一段程序，它可以在未经用户许可，甚至在用户不知情的情况下改变计算机的运行方式。病毒必须满足如下两个条件。

（1）必须能自行执行。它通常将自己的代码置于另一个程序的执行路径中。

（2）必须能自我复制。病毒代码的明确目的是自我复制。例如，它可能用受病毒感染的文件副本替换其他可执行文件。病毒既可以感染桌面计算机也可以感染网络服务器。

与蠕虫相比，病毒可破坏计算机硬件、软件和数据。

2. 蠕虫的特点

蠕虫属于计算机病毒的子类，所以也称为“蠕虫病毒”。通常，蠕虫的传播无需人为干预，并可通过网络进行自我复制，在复制过程中可能有改动。与病毒相比，蠕虫可消耗内存或网络带宽，并导致计算机停止响应。

与病毒类似，蠕虫也在计算机与计算机之间自我复制，但蠕虫可自动完成复制过程，因为它接管了计算机中传输文件或信息的功能。一旦计算机感染了蠕虫，蠕虫即可独自传播。但最危险的是，蠕虫可大量复制。例如，蠕虫可向电子邮件地址簿中的所有联系人发送自己的副本，联系人的计算机也将执行同样的操作，结果造成多米诺效应（网络通信负担沉重），业务网络或整个局域网的速度都将减慢。一旦新的蠕虫被释放，传播速度将非常迅速。蠕虫不仅会使网络堵塞，还会使用户的上网速度变慢。

与病毒相比，蠕虫的传播不必通过“主机”程序或文件，因此蠕虫可潜入用户的系统并允许其他用户或程序远程操控由蠕虫感染的计算机。例如，MyDoom 蠕虫可打开受感染系统的“后门”，然后使用这些系统对网站发起攻击。

蠕虫是不使用驻留文件即可在系统之间复制自身的程序。这点与病毒不同，病毒需要传播受感染的驻留文件。尽管蠕虫通常存在于其他文件（通常是 Word、Excel 等）内部，但蠕虫和病毒使用驻留文件的方式不同。通常，蠕虫将发布其中已包含“蠕虫”宏的文档。这样，整个文档将在计算机之间传播，所以应将整个文档视为蠕虫。

蠕虫的前缀一般是 Worm。这种病毒的公有特性是通过网络或计算机系统漏洞进行传播，大部分的蠕虫都有向外发送带毒邮件，阻塞网络的特性。比如冲击波和震荡波（阻塞网络），小邮差（发带毒邮件）等。

3. 木马的特点

木马的全称为“特洛伊木马”，它是具有欺骗性的文件(宣称是良性的，但事实上是恶意的)。在神话传说中，特洛伊木马表面上是“礼物”，但实际却藏匿了大量袭击特洛伊城的希腊士兵。现在，特洛伊木马是一些表面有用的程序，但实际目的是危害计算机安全性并破坏计算机系统。所以，可以将木马定义为：一种表面有用，但实际有破坏作用的计算机程序。

木马与病毒的重大区别是木马并不像病毒那样复制自身。木马包含能够在触发时导致数据丢失甚至被窃的恶意代码。要使木马传播，必须在计算机上有效地启用这些程序，例如打开电子邮件附件等。

目前，木马主要通过两种途径进行传播：电子邮件和文件下载。一旦用户禁不起诱惑打开了自认为安全的电子邮件的附件，木马便会趁机传播。例如，为了更好地保护用户的系统，现在许多公司或用户通过电子邮件给用户发送安全公告时都不包含附件，例如微软公司的安全公告等。另外，木马也可能包含在免费下载软件中，所以用户在 Internet 上下载了免费软件后，在安装之前一定要进行安全检查。对于安全要求较高的计算机，建议不要安装从 Internet 上直接下载的软件。

木马的前缀是 Trojan。木马的公有特性是通过网络或者系统漏洞进入用户的系统并隐藏，然后向外界泄露用户的信息。木马和黑客软件往往是成对出现的，即木马负责侵入用户的计算机，而黑客软件则会通过该木马来进行控制。

对于 Windows 用户来说，为了有效地防止木马，还需要经常利用 Microsoft Update 或 Microsoft Office Update 下载 Microsoft 更新程序或修补程序。

需要注意的是，病毒、蠕虫与木马之间存在着一定区别，但由于它们都对计算机及网络系统产生危害和威胁，所以人们将三者统称为“计算机病毒”或“病毒”。为此，在本章随后的内容介绍中，也会出现“蠕虫病毒”和“木马病毒”的提法。

6.1.5 计算机病毒的演变过程

20 世纪 80 年代早期出现了第一批计算机病毒。这些病毒的工作原理相对比较简单，一般是自行文件的复制，并在执行时显示简单的恶作剧而已。

1986 年，媒体报道了攻击 Microsoft MS-DOS 个人计算机的第一批病毒，人们普遍认为 Brain 病毒是这些计算机病毒中的第一种病毒。同时出现的病毒还包括 Virdem(第一个文件病毒)和 PC-Write(第一个木马)，在 PC-Write 中木马程序伪装成一个同名的字处理应用程序。

随着更多的人开始研究病毒技术，病毒的数量、被攻击的平台类型及病毒的复杂性和多样性都开始显著提高。病毒在某一时期曾经主要感染启动扇区，然后又开始感染可执行文件。1988 年出现了第一个通过 Internet 传播的蠕虫病毒 Morris Worm，它曾导致 Internet 的通信速度大大地降低。

从 1990 年开始，Internet 的应用为计算机病毒编写者提供了一个可实现快速交流的平台，一些典型的计算机病毒便是大量病毒编写者“集体智慧的结晶”。同年，开发出了第一个多态病毒(通常称为 Chameleon 或 Casper)。多态病毒是指每次传染产生的病毒副本在外观形态上都发生变化的病毒。因此，多态病毒在外观形态上没有固定的特征码。由于多态

病毒具有在每次复制时都可以更改其自身的能力,这使得当时用于“识别”病毒的基于签名的防病毒软件程序很难检测出这种病毒。此后不久,即出现了 Tequila 病毒,这是出现的第一个比较严重的多态病毒攻击。接着在 1992 年,出现了第一个多态病毒引擎和病毒编写工具包。

从此开始,病毒就变得越来越复杂。病毒开始访问电子邮件通信簿,并将其自身添加到通信簿中;宏病毒将其自身附加到各种办公软件的应用程序文件(主要是微软 Office 系列文件)并攻击这些文件。此外还出现了专门利用操作系统和应用程序漏洞的病毒。电子邮件、对等(P2P)文件共享网络、网站、共享驱动器产品漏洞和网络设备(主要有交换机、路由器等)的地址表,都为病毒复制和攻击提供了平台。在已感染系统上创建的后门使得病毒编写者(或黑客)可以返回和运行他们所选择的任何软件。

有些病毒附带其自身的嵌入式电子邮件引擎,可以使已感染的系统直接通过电子邮件传播病毒,而绕过此用户的电子邮件客户端或服务器中的相关设置。病毒编写者还开始认真地设计病毒攻击的结构并开发具有可信外观的电子邮件。这种方法旨在获取用户的信任,使其打开附加的病毒文件,来显著地增加大规模感染的可能性。

随着计算机和网络的普遍使用,计算机病毒技术也在飞速发展,各种新病毒也在层出不穷。从 1986 年 Brain 病毒通过 5.25 英寸软盘首次大规模感染计算机起,人们与计算机病毒的斗争就从未停止过。现在的计算机病毒不但种类繁多,而且危害性不断加强,同时病毒开发工具多种多样,且对开发者的技术要求明显降低。例如,2006 年年底曾轰动一时的“熊猫烧香”病毒的制作者“武汉男孩”李俊只是一名中专毕业生,且在求职中多次受挫。

6.2 蠕虫的清除和防治方法

对于病毒、蠕虫和木马之间的主要区别,在本章前面已经进行了介绍。从本节开始,将分类介绍各类计算机病毒的特征及防治方法。本节首先介绍蠕虫的清除和防治方法。

6.2.1 蠕虫的特征

蠕虫(Worm)是通过分布式网络来扩散特定的信息,进而造成正常的网络服务遭到拒绝并发生死锁的程序。

计算机网络系统的建立是为了使多台计算机能够共享数据资料和外部资源,然而也给计算机蠕虫带来了更为有利的生存和传播的环境。在网络环境下,蠕虫可以按指数增长模式进行传染。蠕虫侵入计算机网络,可以导致计算机网络效率急剧下降、系统资源遭到严重破坏,短时间内造成网络系统的瘫痪。在网络环境中,蠕虫具有如下一些新的特性。

1. 传播速度快

在单机上,病毒只能通过软盘或 U 盘等可移动存储介质从一台计算机传染到另一台计算机,而在网络中则可以通过网络通信机制,借助高速通信网络进行迅速扩散。由于蠕虫在网络中传染速度非常快,使其扩散范围很大,不但能迅速传染局域网内所有计算机,还能通过 Internet 将蠕虫在一瞬间传播到千里之外。

2. 清除难度大

在单机中,再顽固的病毒也可通过删除带毒文件、低级格式化硬盘等措施将病毒清除,而网络中只要有一台主机未能清除干净就可使整个网络重新全部被病毒感染,甚至刚刚完成清除工作的一台主机马上就能被网上另一台主机的带毒程序所传染。因此,仅对主机进行病毒清除不能彻底解决网络蠕虫的问题,而需要借助防火墙等安全设备进行管理。

3. 破坏性强

网络中蠕虫将直接影响网络的工作状态,轻则降低速度,影响工作效率,重则造成网络系统的瘫痪,破坏服务器系统资源,使系统数据毁于一旦。例如,目前在局域网中泛滥的ARP欺骗便属于蠕虫。

6.2.2 蠕虫的分类和主要感染对象

由于蠕虫的最重要特征是它本身就是一个独立的个体,不需要依附于其他程序上,而且自身能够进行复制和传播,同时它以网络作为传播途径来感染计算机。

1. 蠕虫的分类

将“蠕虫”称为“蠕虫病毒”,是因为蠕虫具有病毒的一些共性,如传播性、隐蔽性和破坏性等。同时,蠕虫不同于其他的病毒,是因为它具有自己的一些特征,如不利用文件寄生(即没有宿主程序),在IP网络中利用系统的漏洞进行扫描和入侵,导致网络被阻塞,以及和黑客技术相结合对网络进行攻击等。另外,从破坏性上看,由于蠕虫利用了现代计算机网络的特点,可以在很短时间内蔓延到整个网络,造成网络瘫痪。所以,蠕虫的破坏性是其他病毒所无法比拟的。

根据蠕虫对系统进行破坏的过程,可以将蠕虫分为两类:一类是利用系统漏洞进行攻击,对整个网络(包括企业内部网络和互联网)产生威胁,可造成网络瘫痪。主要有红色代码、尼姆达和sql蠕虫王等;另一类是通过电子邮件及恶意网页的形式进行,主要针对个人用户。主要有爱虫病毒、求职信病毒等。其中,前一类蠕虫具有很大的主动攻击性和突发性,但由于它主要利用系统的漏洞对网络进行破坏,所以这类蠕虫的清除和防治并不困难。第二类病毒的传播方式比较复杂和多样,多利用微软应用程序的漏洞和社会工程学对用户进行欺骗和诱使,所以这类病毒较难完全根除。除两类典型的蠕虫外,目前还存在着一类利用TCP/IP网络协议的缺陷而出现的蠕虫,如ARP欺骗、DHCP欺骗等,这些内容已在本书第5章专门进行了介绍。

2. 蠕虫的感染对象

蠕虫一般不依赖于某一个文件,而是通过IP网络进行自身复制。例如,病毒的传染能力主要是针对计算机内的文件系统而言,而蠕虫的传染目标是网络内的所有主机,例如局域网中的共享文件夹、电子邮件、恶意网页及存在一定漏洞的主机(多为服务器和交换机)等都成为蠕虫传播的主选途径。

6.2.3 系统感染蠕虫后的表现

当蠕虫感染计算机系统后,表现为:系统运行速度和上网速度均变慢,如果网络中有防火墙,防火墙会产生报警等。下面,根据不同类型蠕虫的传播和破坏方式,分别介绍几类主要的蠕虫及系统感染该类蠕虫后的表现。

1. 利用系统漏洞进行破坏的蠕虫

此类蠕虫主要有红色代码、尼姆达和求职信等，它们利用 Windows 操作系统中 IE 浏览器的漏洞（Iframe Execcomand），当通过 Web 方式接收邮件时，使得感染了“尼姆达”病毒的邮件，即使用户不打开它的附件，该类病毒也能够被激活，进而对系统进行破坏。“红色代码”则是利用了 Windows 操作系统中 IIS 的漏洞（idq. dll 远程缓存区溢出）来传播。而“Sql 蠕虫王”是利用了 Microsoft 公司的 SQL Server 数据库系统的漏洞进行大肆攻击。

如 2003 年 8 月 11 日开始出现的冲击波病毒。病毒运行时会不停地利用 IP 扫描技术寻找网络上系统为 Windows 2000 或 Windows XP 的计算机，找到后就利用 DCOM RPC 缓冲区漏洞攻击该系统，一旦攻击成功，病毒体将会被传送到对方计算机中进行感染，使系统操作异常、频繁重启（如图 6-1 所示），甚至导致系统崩溃。另外，该病毒还会对微软的一个升级网站进行拒绝服务攻击，导致该网站堵塞，使用户无法通过该网站升级系统。

再如 2004 年 5 月 1 日出现的“震荡波（Worm. Sasser）”病毒。震荡波病毒主要感染 Windows 2000/XP/2003 等操作系统的计算机，感染震荡波病毒的系统将开启上百个线程去攻击其他网上的用户，可造成机器运行缓慢、网络堵塞，并让系统不停地进行倒计时重启，如图 6-2 所示。其中毒现象非常类似于“冲击波”。



图 6-1 Windows 操作系统感染冲击波病毒后显示的关机界面



图 6-2 Windows 操作系统感染“震荡波”病毒后显示的关机界面

2. 通过网页进行触发的蠕虫

蠕虫的编写技术与传统的病毒有所不同，许多蠕虫是利用当前最新的编程语言与编程技术来编写的，而且同一蠕虫程序易于修改，从而产生新的变种，以逃避反病毒软件的搜索。现在大量的蠕虫用 Java、ActiveX 和 VB Script 等技术，多潜伏在 HTML 页面文件里，当打开相应的网页时则自动触发。

3. 蠕虫与黑客技术相结合

现在的许多蠕虫不仅仅是单独对系统破坏，而是与黑客技术相结合，为黑客入侵提供必要的条件。例如当系统感染“红色代码”后，在计算机的 Web 目录的\scripts 子目录下将生成一个 root. exe，利用该文件可以远程执行任何命令，从而使黑客能够再次进入。

另外，像“尼姆达”、“求职信”等蠕虫可通过文件、电子邮件、Web 服务器和网络共享等多种途径进行传播。表 6-1 列出了一些主要的蠕虫及产生的损失情况。

表 6-1　一些主要蠕虫及产生的损失情况

蠕虫名称	发作时间	造成损失
莫里斯蠕虫	1988 年	这是世界上第一个蠕虫，造成 6000 多台计算机停机，直接经济损失达 9600 万美元
美丽杀手	1999 年	政府部门和一些大公司紧急关闭了网络服务器，经济损失超过 12 亿美元
爱虫病毒	2000 年	众多用户计算机被感染，损失超过 100 亿美元
尼姆达	2001 年	利用电子邮件、IIS 和网上邻居等多种途径对网络产生阻塞，感染主机在 800 万台以上，造成经济损失 6 亿多美元
红色代码	2001 年 7 月	网络瘫痪，直接经济损失超过 26 亿美元。这也是首个黑客病毒
求职信	2001 年 12 月	大量病毒邮件堵塞服务器，损失达数百亿美元
SQL 蠕虫王	2003 年 1 月	网络大面积瘫痪，银行自动提款机运作中断，直接经济损失超过 26 亿美元
冲击波	2003 年	首个利用微软公司公布的系统漏洞发动恶性攻击的蠕虫，利用计算机网络在一夜之间造成 1000 多台主机感染，直接经济损失 100 亿美元
震荡波	2004 年	是继冲击波后，利用微软公司公布的系统漏洞发动恶性攻击的另一个蠕虫。直接经济损失与冲击波发作时基本相当

6.2.4　实验操作 1　蠕虫的防治方法

如果说病毒的清除是当务之急，那么病毒的防治则是居安思危。防患于未然是每一位网络管理人员应该养成的良好习惯。本小节将具体介绍蠕虫的防治方法。

1. 更新系统补丁

更新系统补丁的目的之一是堵住系统的漏洞。前面介绍的 SQL 蠕虫王、冲击波和震荡波病毒都是利用系统存在的不同漏洞来入侵并发作的，所以及时更新补丁对于防治蠕虫是非常重要的。

针对 Windows 操作系统的漏洞，各类杀病毒软件一般都提供了漏洞扫描功能，同时也有一些专门的漏洞扫描软件。但是，最有效和方便的方法是利用 Windows 操作系统自带的 Windows Update 补丁管理工具来为系统安装补丁程序。对于企业用户，可以部署 WSUS 补丁更新服务器，对局域网内部的计算机统一更新系统补丁。

Windows Update 分为在线更新和自动更新两种方法。其中，在线更新需要将安装补丁程序的计算机接入 Internet，在 IE 浏览器中输入 Microsoft 公司补丁程序网站的地址 http://windowsupdate.microsoft.com，或在 IE 浏览器中选择"工具"→windows update 命令来打开在线更新功能。当用户打开在线更新功能时，系统本身会把自己的相关信息上传给补丁程序更新网站，然后网站根据收到的系统信息判断系统有哪些补丁程序还没有安装，并且将结果以列表的形式显示出来，如图 6-3 所示。用户可以在该列表中选择要安装的补丁程序。

对于单位的网络管理人员来说，由于管理的机器较多，可能会忘记给每一台机器及时地安装补丁程序，这时就可以使用自动更新功能。Windows update 自动更新功能的使用方法为：选择"开始"→"设置"→"控制面板"→"自动更新"命令，在打开的如图 6-4 所示的对话框中进行配置，其中需要选择"自动(推荐)"单选按钮，然后在下方的下拉列表中选择自动更

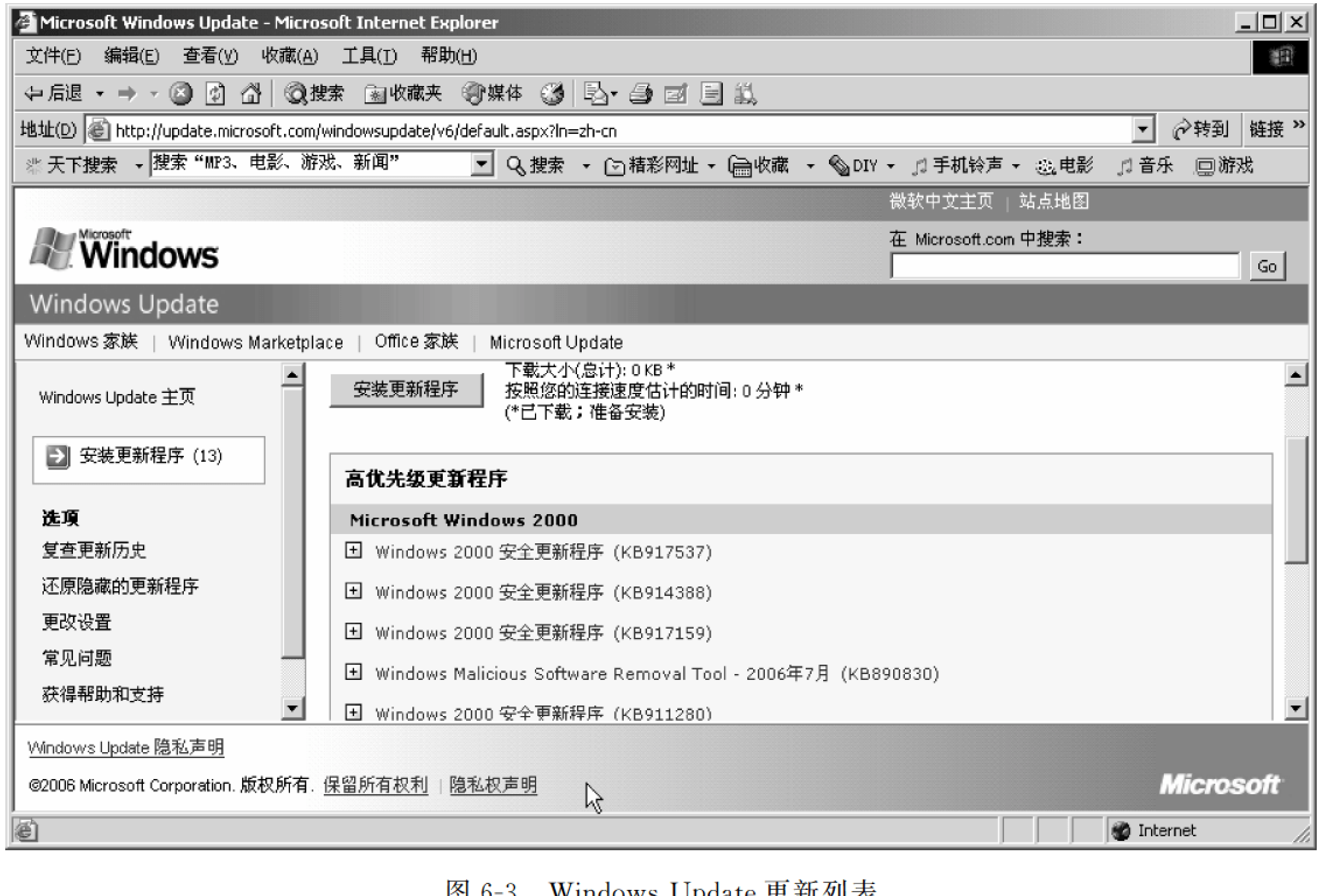


图 6-3 Windows Update 更新列表

新的时间。一般建议系统每天都要进行更新，但更新的时间可以放在机器和网络都比较空闲的时候，如夜里 1:00。这样，系统会在用户指定的时间自动到 Windows Update 网站下载并安装最新的补丁程序。

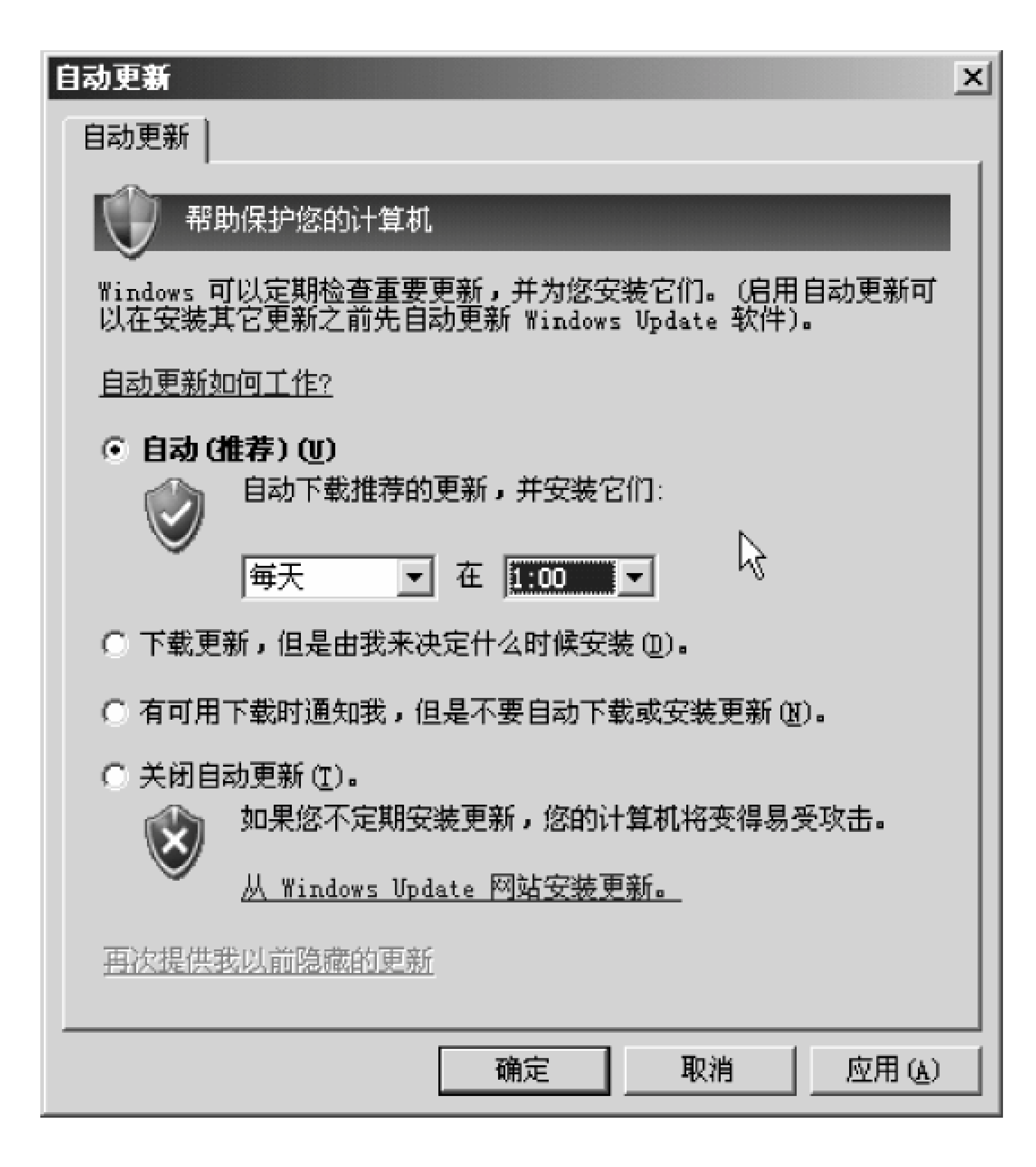


图 6-4 Windows update 的自动更新配置对话框

除自动更新之外，系统还提供了“下载更新”和“下载通知”两个功能。如图 6-4 所示，如果选择了“下载更新，但是由我来决定什么时候安装”单选按钮，系统会随时到 Windows

Update 网站下载补丁程序，之后会提示用户是否要安装该补丁程序；当选择了“有可用下载时通知我，但是不要自动下载或安装更新”单选按钮时，如果 Windows Update 网站有新的补丁发布，系统会提示用户来下载并安装该补丁程序，如图 6-5 所示。用户可以选择“快速安装(推荐)”单选按钮来安装所有的补丁程序，也可以选择“自定义安装(高级)”单选按钮来选择安装部分补丁程序。



图 6-5 “自动更新”操作对话框

2. 加强对系统账户名称及密码的管理

现在的一些蠕虫已经具备了黑客程序的一些功能，有些蠕虫会通过暴力破解的方法来获得系统管理员的账户名称和密码，从而以系统管理员的身份来入侵系统，并对其进行破坏。为此，必须加强对系统管理员账户及密码的管理。

Windows 2000/XP/2003 默认的系统管理员账户名称为 Administrator，为了防止蠕虫轻而易举地获得该账户名称，建议用户将 Administrator 进行更名(如 Admin-jsnj)，如图 6-6 所示。



图 6-6 对 Administrator 进行重命令操作

为了加强系统的安全性，Windows Server 2003 对账户密码设置进行了严格要求，但 Windows XP 和 Windows 2000 并不具备此功能。为此，对于 Windows XP 和 Windows 2000 来说，必须加强对账户密码的管理。对于密码的设置，建议使用“四纬空间”规则，“四纬空间”分别为小写字母、大写字母、数字和特殊字符（如 &、/等）4 类符号，即每个账户的密码中应同时包括这 4 类符号，同时密码的长度应在 8 位以上。

据相关数字统计，一个密码前 6 位的安全性是非常重要的。为此，建议用户在设置密码尤其是系统管理员账户的密码时，其前 6 位一定要使用“四纬空间”规则。

另外，如果没有特殊要求，建议不要在系统中创建太多的账户，尤其是与 Administrator 具有相同权限的管理员账户。对于 Guest 账户，在不需要的时候可将其停用或直接删除。但是，在有些时候 Guest 账户是不能停用的，如设置了文件共享时，就需要用户 Guest，否则其他用户将无法访问该共享文件。

对于 Administrator 和 Guest 账户，除设置较为复杂的密码外，还有一个方法能够让 Administrator 和 Guest 调换其身份。具体方法是选择“开始”→“运行”命令，在打开的对话框中输入 gpedit. msc。单击“确定”按钮后，在打开的“组策略”窗口中选择“Windows 设置”→“本地策略”→“安全选项”，在右侧窗口中将会显示“重命名来宾账户”和“重命名系统管理员账户”两项，如图 6-7 所示。

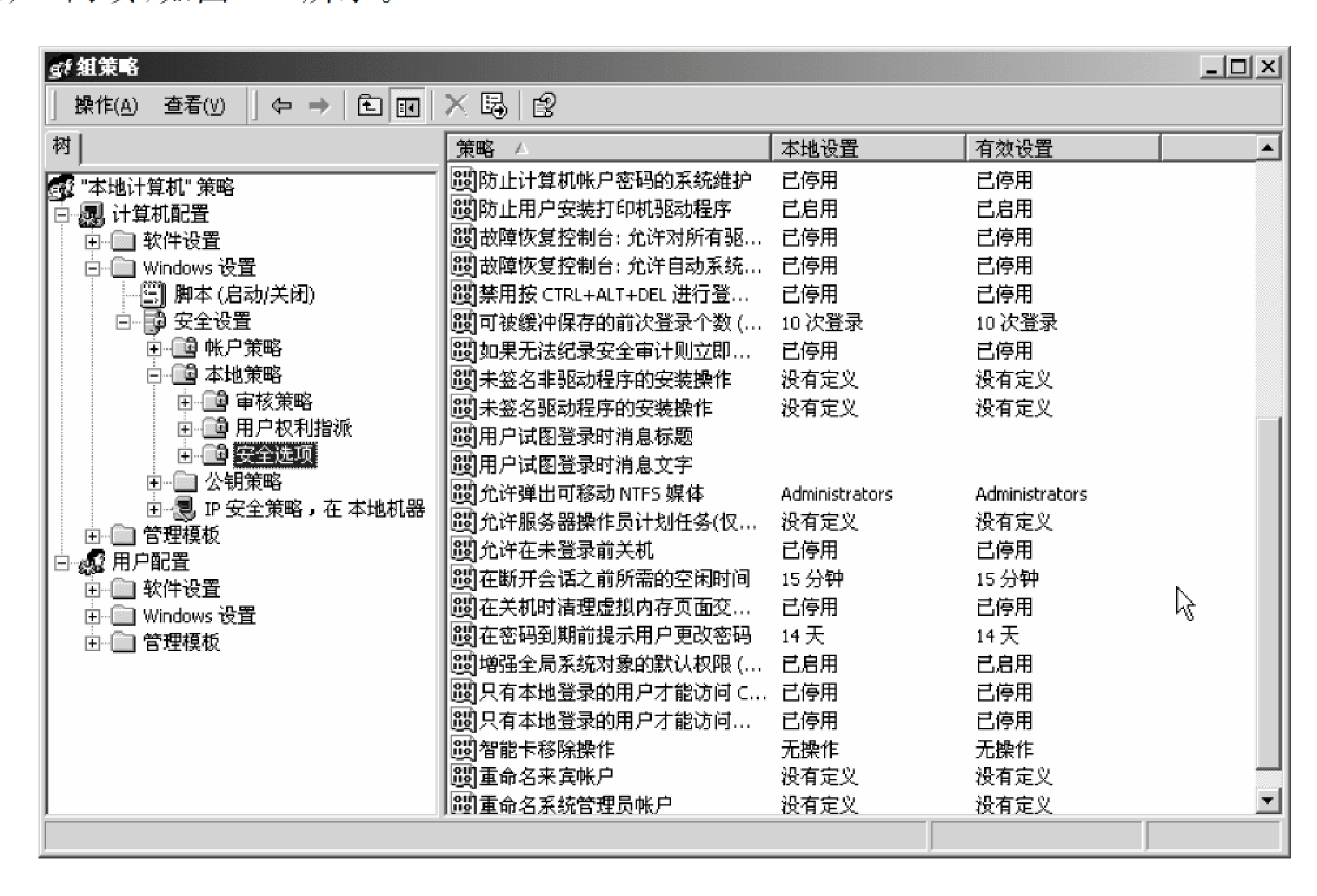


图 6-7 组策略设置窗口

利用这两个策略，用户可以把系统管理员 Administrator 的账户名称更改为 Guest，而将来宾账户 Guest 的名称更改为 Administrator。通过这样的设置，就会给蠕虫设置一个陷阱，即使有蠕虫获得了 Administrator 的密码，当其入侵系统后也只能从事来宾账户的操作，对系统产生的危害相应要小一些。

3. 取消共享连接

文件和文件夹共享及 IPC（ Internet Process Connection）连接是蠕虫常使用的入侵途

径。所以，为了防止蠕虫入侵，建议关闭不需要的共享文件或文件夹及 IPC，如图 6-8 所示。



图 6-8　显示已存在的共享设置

具体方法是：选择"开始"→"运行"命令，在打开的对话框中输入 services. msc 命令，单击"确定"按钮，打开"服务"窗口。在该窗口中找到 Server 服务，单击鼠标右键，在弹出的快捷菜单中选择"停止"命令，将打开如图 6-9 所示的对话框。单击"是"按钮，将关闭所有的共享服务，这样原来在图 6-8 中所示的共享连接将无法使用。

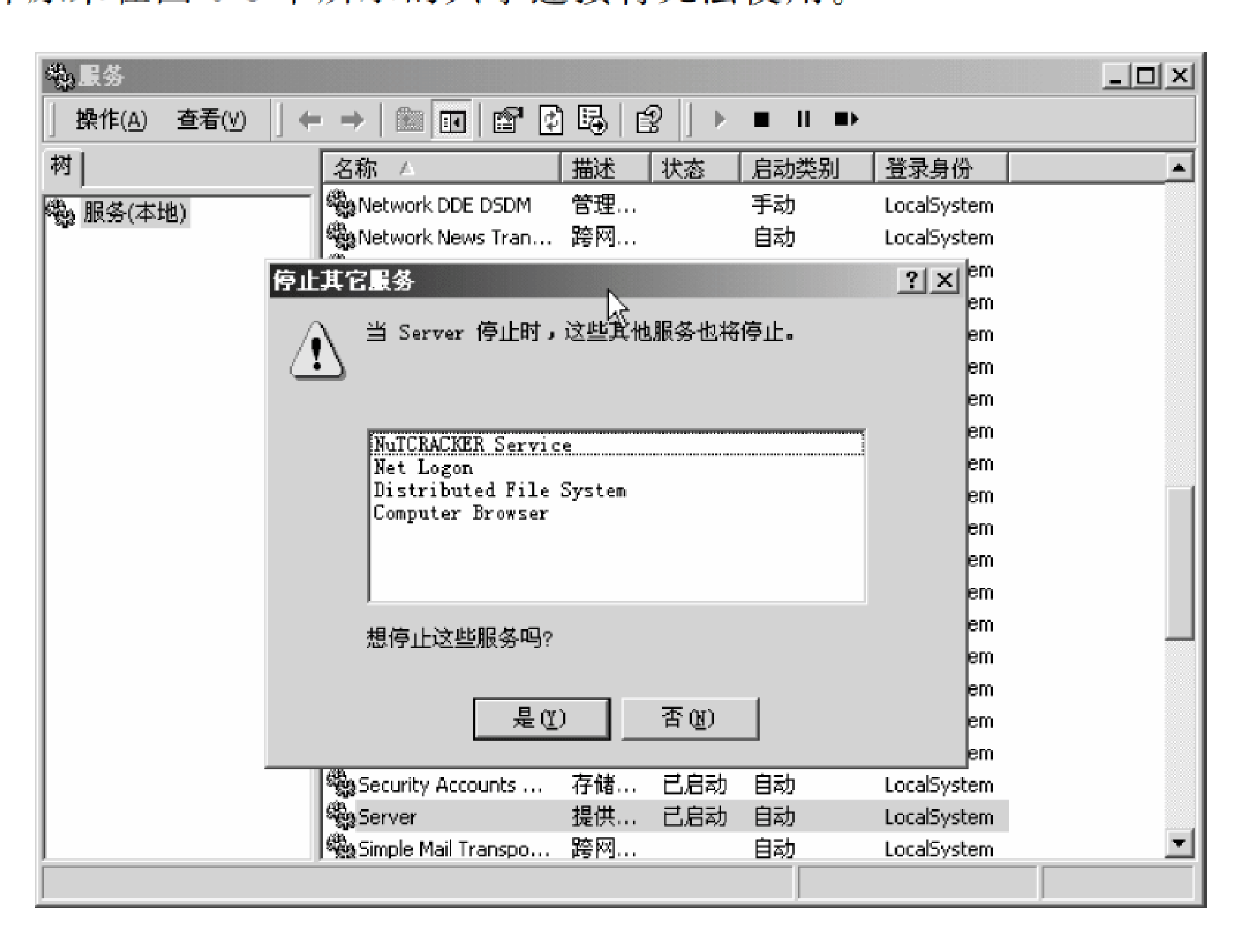


图 6-9　停止 Server 服务

在局域网中如果确实要通过共享来访问某些资源，这时可以通过设置访问者及其权限来增强共享安全性。以 soft 文件夹为例，方法是：在"soft 属性"对话框中选择"共享"选项卡（如图 6-10 所示），单击"权限"按钮，将打开如图 6-11 所示的"soft 的权限"对话框。其中，系统默认是每一个用户（Everyone）都能够访问该共享资源，而且访问权限是"完全控制"。为了加强共享的安全性，可以将 Everyone 账户删除，然后单击"添加"按钮，添加允许访问该共享资源的用户名，同时可以根据用户实际需求来设置相应的权限。例如，只需要通过网络

访问该共享文件夹下的文件时,可以将权限设置为“读取”即可。




图 6-10　设置文件夹的共享属性



图 6-11　设置访问者的账户名称和权限

另外,由于一些蠕虫直接利用脚本语言来编写,所以为了避免蠕虫的入侵,可以删除基于窗口和命令行的两个脚本解释器 WScript.exe 和 CScript.exe,这部分内容将在 6.3 节进行介绍。同时,为了防止蠕虫通过 IE 浏览器入侵用户的系统,可以在 IE 安全设置中将 ActiveX 控件和 Java 脚本删除。还有,像冲击波和震荡波等利用端口进行入侵和传播的蠕虫,可以在防火墙上关闭其端口,如 TCP 135、TCP 4444、UDP 69、TCP 5554、TCP 445 和 TCP 9996 等。

6.3　脚本病毒的清除和防治方法

脚本(Script)是使用一种特定的描述性语言,依据一定的格式编写的可执行文件,又称作宏或批处理文件。脚本通常可以由应用程序临时调用并执行。因为脚本不仅可以减小网页的规模和提高网页浏览速度,而且可以丰富网页的表现(如动画、声音等),所以各类脚本目前被广泛地应用于网页设计中。也正因为脚本的这些特点,所以往往被一些别有用心的人所利用。例如在脚本中加入一些破坏计算机系统的命令或直接植入木马等,这样当用户浏览网页时,一旦调用这类脚本,便会使用户的系统受到攻击。本节将介绍脚本病毒的特征和防治方法。

6.3.1　脚本的特征

脚本语言能够嵌入到 HTML 文件中,同时具有解释执行功能。根据脚本语言的工作原理,可以将其分为两大类:服务器端脚本和客户端脚本。

(1) 服务器端脚本。是指由 Web 服务器负责解释执行的脚本,客户端的浏览器只需要显示服务器端的执行结果。ASP、PHP 和 JSP 是常用的服务器端脚本语言。

(2) 客户端脚本。是指由浏览器负责解释执行的脚本。常见的客户端脚本语言有

Visual Basic Script(VBS)语言和 Java Script(JS)语言。

Visual Basic Script 语言是在 Microsoft Visual Basic 语言的基础之上开发的,能够嵌入 HTML 中的脚本语言,其特点是易学易用;而 Java Script 是一种基于对象(Object)和事件驱动(Event Driven)的,并具有安全性能的脚本语言。Java Script 主要用于 HTML 页面,其源码可直接嵌入到 HTML 中。用 Java Script 编写的程序不必在运行前编译,它可以直接写入 Web 页面中,并由调用它的浏览器来解释执行,以提高客户端的响应时间。

正是由于脚本语言具有以上的特征,所以现在大量的 Web 页面都嵌入了脚本语言,同时越来越多的网络应用使用脚本语言来编写。也正是如此,一些别有用心的用户便使用脚本语言来编辑病毒程序(即脚本病毒),并通过网络进行传播。

6.3.2 脚本病毒的特征

脚本病毒主要是由 Visual Basic Script 语言和 Java Script 语言来编写的计算机病毒,可以直接添加到同类的程序代码(如 HTML)中,通过调用 Windows 组件或对象,直接对注册表、文件系统进行操作。

脚本病毒的传播途径比较多,由于 Visual Basic Script 和 Java Script 编写的代码可以直接插入到 HTML 文件中,同时浏览器也直接支持对这两种语言所编写代码的解释,所以脚本病毒多通过 Web 页面进行传播,也可以经常插入到电子邮件的附件或通过局域网的共享设置来传播。总的来说,脚本病毒具有以下特点。

(1) 编写简单。即使一个以前对病毒一无所知的用户,只要略懂 HTML、Visual Basic Script 和 Java Script 语言的编写方法,就可以在很短的时间里编写出一个新型病毒来。例如,下面就是一段通过使用脚本语言显示当前时间的代码。用户只需要使用任何一个文本编辑器来输入这段代码,并保存为以 HTML 为扩展名的文件,当利用浏览器打开时就会直接执行,结果如图 6-12 所示。



图 6-12 一个显示当时时间的脚本

```
<tr><TD width = 210 align = "center"><font color = "#0000FF">
<SCRIPT language = JavaScript>
today = new Date();
function initarray(){
this.length = initarray.arguments.length
for(var i = 0;i<this.length;i ++ )
this[i + 1] = initarray.arguments[i] }
var d = new initarray(
" 星期日 ",
" 星期一 ",
" 星期二 ",
" 星期三 ",
" 星期四 ",
```

```
" 星期五 ",
" 星期六 ");
document.write(
today.getYear(),"年",
today.getMonth() + 1,"月",
today.getDate(),"日",
d[today.getDay() + 1]);
</SCRIPT>
</font></TD></tr>
```

(2) 破坏力大。脚本病毒的破坏力不仅表现在对用户系统文件的破坏,还可以使邮件服务器崩溃,网络发生严重阻塞。

(3) 感染力强。由于脚本是直接解释执行,同时它不像其他病毒那样需要做复杂的文件格式处理,因此脚本病毒可以直接通过自我复制的方式感染其他同类文件。

(4) 病毒源代码容易被获取,且变种较多。由于 VBS(Visual Basic Script)和 JS(Java Script)病毒直接解释执行,其源代码的可读性非常强,即使病毒源代码经过加密处理,其源代码的获取还是比较简单。因此,这类病毒变种比较多,稍微改变一下病毒的结构,或者修改一下特征值,就会使很多杀毒软件一时无法发现它。

(5) 欺骗性强。脚本病毒为了能够迷惑用户得以运行,往往会对自己进行必要的伪装。例如,有些插入到电子邮件附件中的脚本病毒,它会使用.jpg.vbs 的后缀。由于 Windows 操作系统在默认情况下不会显示后缀,这样用户看到的将是一个 jpg 图片文件。

正因为以上几个特点,脚本病毒的发展异常迅速,许多新型脚本病毒层出不穷。

6.3.3 实验操作 2 脚本病毒的防治方法

脚本病毒一般通过电子邮件的附件,局域网共享和 HTML、ASP、JSP、PHP 网页等方式传播。在传播过程中,脚本病毒存在以下特点。

(1) 运行时需要 FileSystemObject(文件系统对象)的支持。

(2) 运行时需要通过 Windows 脚本宿主(Windows Scripting Host,WSH)来解释执行。

(3) 运行时需要其关联程序文件 WScript.exe 的支持。

(4) 当通过网页传播时需要 ActiveX 控件的支持。

(5) 当通过电子邮件传播时需要 Outlook 的支持。

在掌握了以上脚本病毒的传播途径后,下面介绍几类脚本病毒的防治方法。

1. 网页脚本病毒的防治

根据微软公司权威软件开发指南 MSDN(Microsoft Developer Network)的定义,ActiveX 控件以前也叫做 OLE 控件或 OCX 控件,它是一些软件组件或对象,可以将其插入到 Web 网页或其他应用程序中。

在因特网上,ActiveX 控件软件的特点是:一般软件需要用户单独在操作系统上进行安装,而 ActiveX 控件是当用户浏览到特定的网页时,IE 浏览器即可自动下载并提示用户安装。ActiveX 控件安装的一个前提是必须经过用户的同意或确认,如图 6-13 所示。

此站点可能需要下列ActiveX 控件：来自 'Beijing 3721 Technology Co., Ltd.' 的 '中文上网 升级包，升级电脑的中文搜索功能， 并帮助您屏蔽恶意网站、修复IE、拦截弹出广告(点...'。单击此处安装...

图 6-13　系统提示是否安装 ActiveX 控件

ActiveX 插件技术是国际上通用的基于 Windows 平台的软件技术，除了网络实名插件之外，许多软件均采用此种方式开发，例如 Flash 动画播放插件、Microsoft Media Player 插件等。

当通过 Internet 发行软件时，软件的安全性是一个非常引人关注的问题，IE 浏览器通过以下方式来保证 ActiveX 插件的安全。

(1) ActiveX 使用了两个补充性的策略：安全级别和证明，来追求进一步的软件安全性。

(2) Microsoft 公司提供了一套工具，可以用来增加 ActiveX 对象的安全性。

(3) 通过 Microsoft 公司的验证代码工具，可以对 ActiveX 控件进行签名，这告诉用户你的确是控件的作者而且没有他人篡改过这个控件。

(4) 为了使用验证代码工具对组件进行签名，必须从证书授权机构获得一个数字证书。证书包含表明特定软件程序是正版的信息，这确保了其他程序不能再使用原程序的标识。证书还记录了颁发日期。当用户试图下载软件时，IE 浏览器会验证证书中的信息，以及当前日期是否在证书的截止日期之前。如果在下载时该信息不是最新的和有效的，IE 浏览器将显示一个警告。

(5) 在 IE 浏览器默认的安全级别中，ActiveX 控件安装之前，用户可以根据自己对软件发行商和软件本身的信任程度，选择决定是否继续安装和运行此软件(如图 6-13 所示)。

网络实名插件使用了国际权威安全厂商 Verisign 所颁发的数字证书进行签名，因此可以确保网络实名插件的真实性和安全性。

网络实名插件通过微软公司 ActiveX 技术来进行安装，单击弹出窗口中的“详细信息”按钮后，微软公司已经告诉用户应该了解的信息(包括数字证书的发行商、有效期和所有者等)，并根据用户单击“是”或“否”按钮来决定是否安装插件。网络实名插件安装时的弹出窗口是 ActiveX 标准的安装界面，是由 Windows 控制的，只能通过单击上面的链接来查看软件详细介绍和使用许可协议等信息。

从组成来看，ActiveX 既包含服务器端技术，也包含客户端技术。其主要内容如下。

(1) ActiveX 控制(ActiveX Control)。用于向 Web 页面、Microsoft Word 等支持 ActiveX 的容器(Container)中插入 COM 对象。

(2) ActiveX 文档(ActiveX Document)。用于在 Web 浏览器(主要是 IE 浏览器)或者其他支持 ActiveX 的容器中浏览复合文档(非 HTML 文档)，例如 Microsoft Word 文档、Microsoft Excel 文档或者用户自定义的文档等。

(3) ActiveX 脚本描述(ActiveX Scripting)。用于从客户端或者服务器端操纵 ActiveX 控制和 Java 程序，传递数据，协调它们之间的操作。

(4) ActiveX 服务器框架(ActiveX Server Framework)。提供了一系列针对 Web 服务器应用程序设计各个方面的函数及其封装类，例如服务器过滤器、HTML 数据流控制等。

在 IE 中内置了 Java 虚拟机(Java Virtual Machine)，从而使 Java Applet 能够在 IE 上

运行，并可以与 ActiveX 控制通过脚本描述语言进行通信。

从上面 ActiveX 的工作原理可以看出，网页脚本病毒与 ActiveX 控件之间存在着一种依赖关系，如果用户在技术上保证了 ActiveX 的安全，也就保证了网页的安全。其实，用户只需要对 IE 自带的安全属性进行必要的配置就可以阻止网页脚本病毒的侵扰。具体配置方法为：在桌面上选取 Internet Explorer，单击鼠标右键，在弹出的快捷菜单中选择“属性”命令，将打开如图 6-14 所示的“Internet 属性”对话框。单击“自定义级别”按钮，在打开的如图 6-15 所示的“安全设置”对话框中设置 ActiveX 控件和插件的属性。从安全方面考虑，对不安全的控件和插件全部设置为“禁用”，同时将“安全级”设置为“高”。



图 6-14 “Internet 属性”对话框

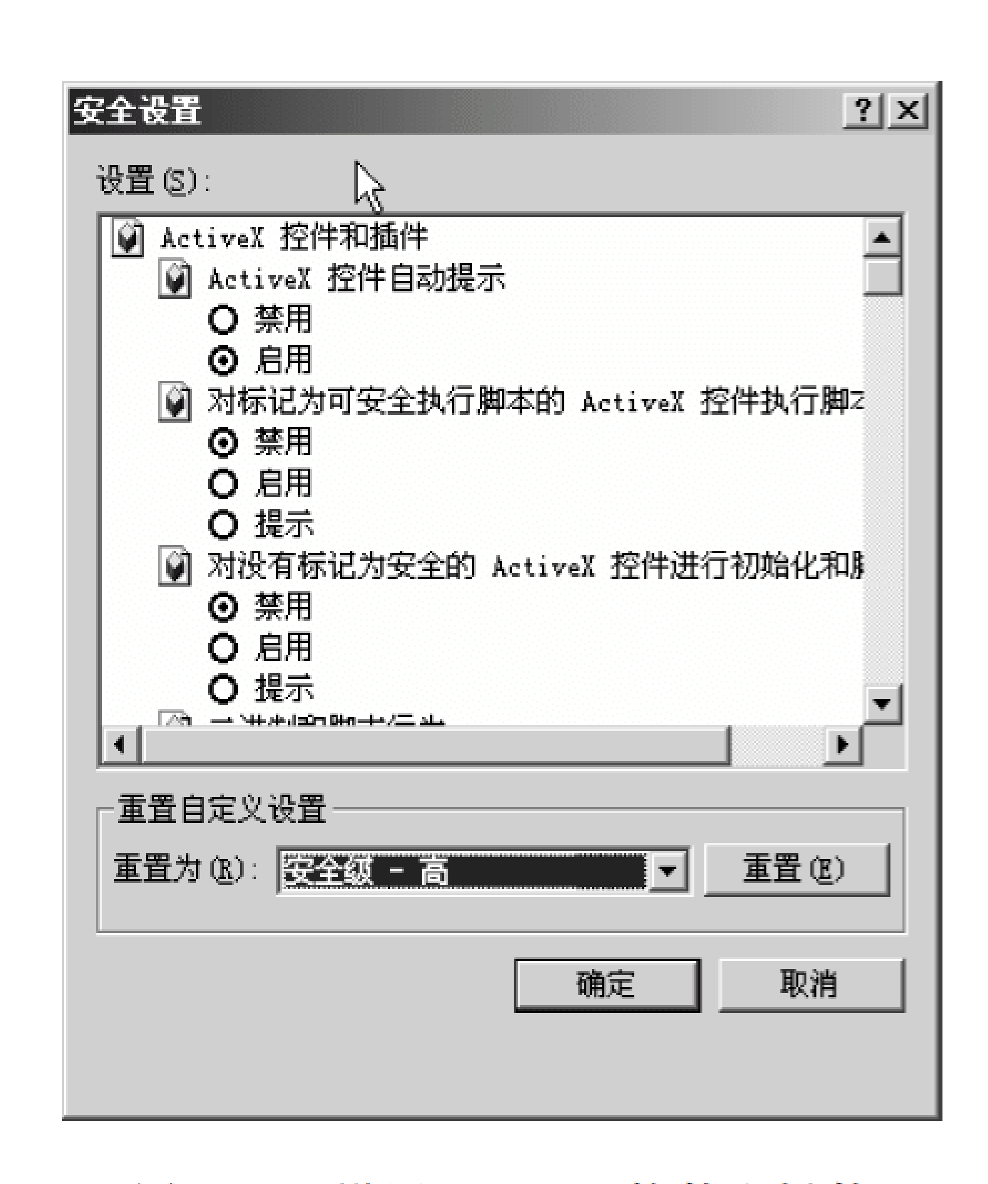


图 6-15 设置 ActiveX 控件和插件

如果将下载 ActiveX 控件和插件的功能全部设置为“禁用”，这样即使浏览了带有脚本病毒的网页，但由于 IE 无法解析和执行这些 ActiveX 控件，这样病毒将找不到执行自身的程序，从而避免了脚本病毒入侵网页。

需要注意的是，如果禁用了 ActiveX 控件，这时当用户浏览带有 ActiveX 控件的网站时，将无法查看和使用一些脚本语言实现的特效。这时，就需要在应用功能与安全之间进行必要的选择。

2. 局域网中脚本病毒的防治

大多数单位组建局域网的主要目的是实现资源共享，而局域网中的资源共享是大多数脚本病毒传输的首选途径。同时，局域网中的脚本病毒很难完全清除，只要有一台计算机未彻底地清除病毒，就会使局域网中的清除病毒工作前功尽弃，当这台未清除病毒的计算机接入局域网后，病毒就会利用网络很快传播开来。

局域网中脚本病毒入侵的方法很简单，脚本病毒主要是利用共享资源的“可写”属性，来将病毒文件放入共享文件夹，或添加到共享文件夹中的文件中。所以，在局域网中预防脚本病毒的方法主要是取消对共享资源的“可写”属性，而将其修改为“只读”，如图 6-16 所示。

另外，在局域网中传播的许多脚本病毒会将自己伪装成为脚本文件，例如病毒文件

love.jpg 文件在传播之前为了避开杀病毒软件的扫描，便将其修改为双扩展名的文件 love.jpg.vbs，而脚本文件 *.vbs 系统默认是隐藏起来的，这样脚本病毒也就“骗过”了用户的检查。为此，在手工清除这类双扩展名的脚本病毒文件时，首先要取消系统默认的隐藏扩展名的设置。具体操作方法为：在打开的文件夹中，选择“工具”→“文件夹选项”→“查看”命令，在打开的如图 6-17 所示的“文件夹选项”对话框中，取消对“隐藏已知文件类型的扩展名”复选框的选取，然后单击“确定”按钮即可。



图 6-16　将共享资源的属性设置为“只读”

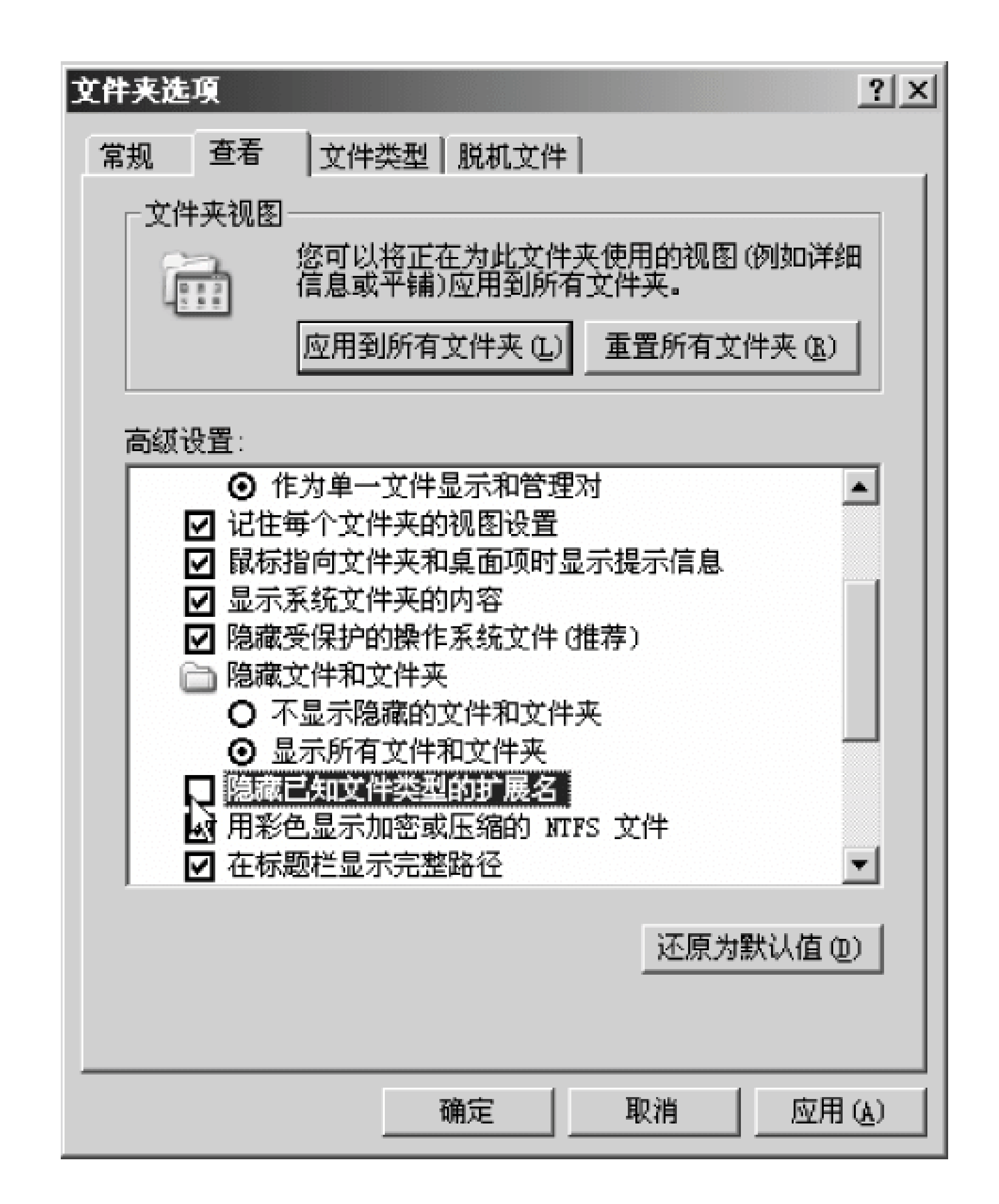


图 6-17　取消对“隐藏已知文件类型的扩展名”复选框的选取

由于脚本病毒在局域网中会利用邮件附件进行传播，所以在局域网中使用邮件系统时，对于来路不明的邮件，建议不要随意打开其附件，否则会导致脚本病毒入侵并破坏用户的计算机系统。对于局域网用户来说，一个良好的习惯是在打开邮件的附件之前，首先将附件下载到指定的磁盘上，然后再利用杀病毒软件对其进行查毒操作，在确认附件没有感染病毒后再打开。

目前在市面上销售的杀病毒软件，只要用户能够及时更新病毒库，一般都能够清除各类脚本病毒（同时也包括其他的计算机病毒）。

6.3.4　实验操作 3　通过管理 WSH 来防治脚本病毒

WSH（Windows Scripting Host，Windows 脚本宿主）是内嵌于 Windows 操作系统中的脚本语言工作环境，它使 Windows 操作系统具备了更为强大的功能，并方便了用户对系统的使用。

1. 认识 WSH

WSH 这个概念最早出现于 Windows 98 操作系统。早期，在 Windows 95 和 DOS 操作系统下，为了方便用户使用、有效地简化工作，多使用批处理命令（如 DOS 操作系统下的 autoexec.bat 文件）。其实，批处理命令有点类似于脚本语言，所以有时也将批处理命令看作是“一种特殊的在 Windows 98 之前的操作系统中支持的脚本语言”。随着 Windows 98

操作系统的问世，同时随着各种真正的脚本语言的不断出现，批处理命令的缺陷越来越明显。为此，微软公司在研发 Windows 98 操作系统时，为了实现多类脚本文件在 Windows 界面或 DOS 命令提示符下的直接运行，就在系统内植入了一个基于 32 位 Windows 平台、并独立于语言的脚本运行环境，并将其命名为 Windows Scripting Host。WSH 架构于 ActiveX 之上，通过充当 ActiveX 的脚本引擎控制器，为 Windows 用户充分利用脚本指令语言提供了保障。

更具体地讲，当用户编写了一个脚本文件(后缀为.vbs 或.js)后，在 Windows 下双击并执行，这时系统就会自动调用一个适当的程序来对它进行解释并执行，而这个程序就是 Windows Scripting Host，程序执行文件名为位于%winroot/system32 文件夹下的 Wscript.exe(如果在命令提示符下，则为 Cscript.exe)文件，如图 6-18 所示。其中%winroot 为 Windows 的安装文件夹。



图 6-18 位于%winroot/system32 文件夹下的 Wscript.exe 文件

2. WSH 内置的对象及功能

WSH 发展到现在，其功能已经十分强大，现在可以利用脚本来完成许多操作，如网络驱动器的映射、环境变量的修改和注册表项的处理等。另外，管理员还可以使用 WSH 来编写脚本实现对 Windows Server 2000 或 Windows Server 2003 活动目录的管理。以上功能的实现，都是 WSH 内置的 14 个对象(如图 6-19 所示)来直接处理脚本指令。具体功能如下。

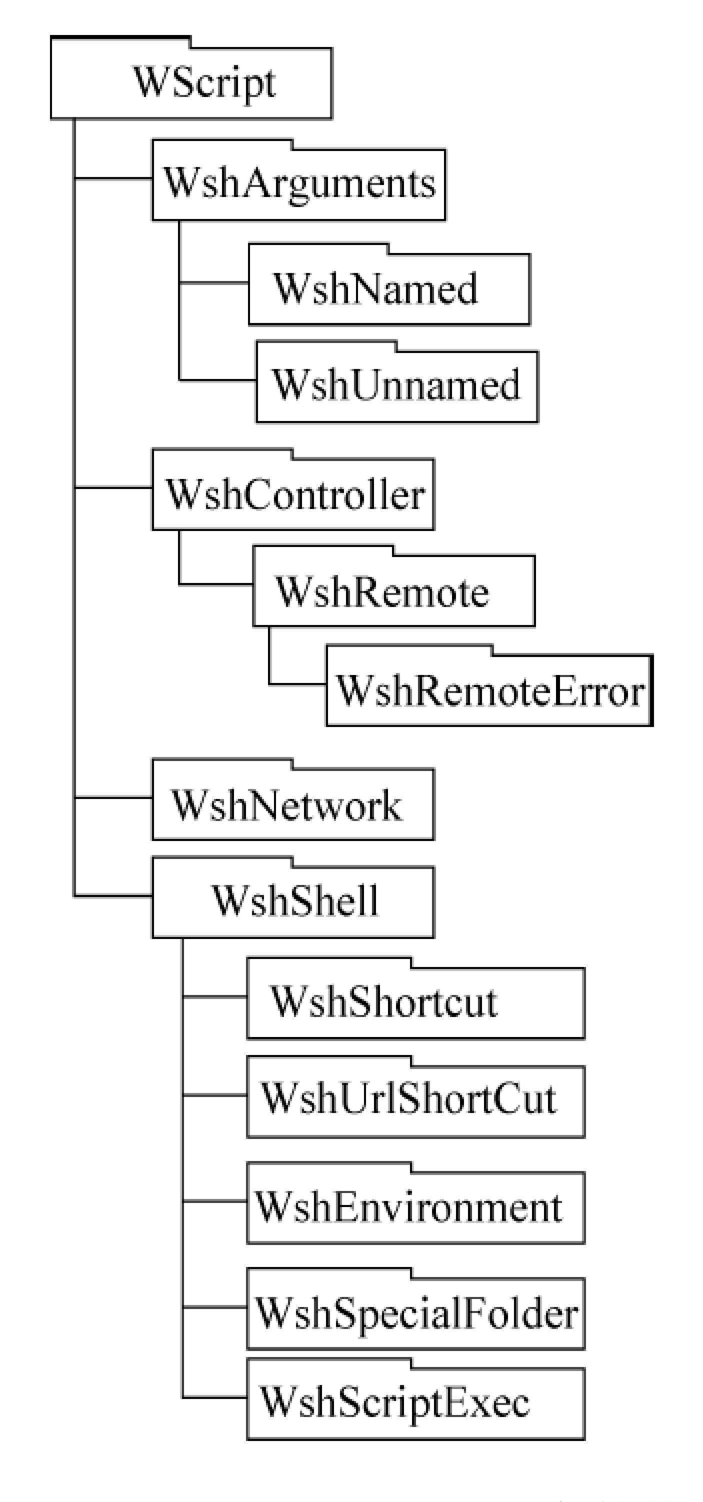


图 6-19 WSH 内置的对象结构

- Wscript：主要作用是提取命令行变量，确定 WSH 执行的文件名是 Sscript.exe 还是 Cscript.exe，以确认 host 的版本信息，以及按程序结束一个脚本文件的运行，并向默认的输出设备(如对话框、命令行等)输出信息等。
- WshArguments：主要作用是获取全部的命令行变量。
- WshNamed：主要负责获取指定的命令行参数集。
- WshUnnamed：主要负责获取未经指定的命令行参数集。

- WshNetwork：主要作用是开放或关闭网络共享，连接或断开网络打印机，获取当前登录用户的信息等。
- WshController：用于创建一个远程脚本对象。
- WshRemote：实现网络中对计算机系统的远程管理，也可按计划对其他程序或脚本进行处理。
- WshRemoteError：主要作用是当一个远程脚本（WshRemote 对象）因脚本错误而终止时，将获取可用的错误信息。
- WshShell：主要负责程序的本地运行，处理注册表项，创建快捷方式，获取系统文件夹信息，处理环境变量等。
- WshShortcut：主要用于按计划创建快捷方式。
- WshSpecialfolders：主要用于获取任意一个 Windows 特殊文件夹的信息。
- WshURLShortcut：主要用于按程序要求创建进入网络地址的快捷方式。
- WshEnvironment：主要用于获取任意的环境变量，如 WINDIR、PATH 和 PROMPT 等。
- WshScriptExec：主要用于确定一个脚本文件的运行状态及错误信息。

通过以上这 14 个 WSH 内置的对象，用户就可以利用 WSH 来使 VBScript 和 JScript 等脚本发挥更大的功能，提高系统的运行效率。

3. WSH 的工作过程

WSH 的工作过程其实就是脚本文件被解析并执行的过程。例如，在现在的 Web 页面（如 HTML、ASP 页面等）中大量地加入了脚本以增强页面的效果，对于添加到 HTML 页面中的脚本，一般需要利用 IE 来解析并运行，而对于添加到 ASP 页面中的脚本，则由 IIS（Internet Information Services）提供解释。

下面举一个 WSH 的应用实例。只需要在“记事本”等文本编辑器中输入以下一行命令：

```
WScript.Echo ("您好！这是 WSH 的一个应用实例")
```

之后，将其保存为一个脚本文件（扩展名为.js 或.vbs），如 wsh.vbs。然后双击 wsh.vbs 文件，将会显示如图 6-20 所示的信息。

由于本节主要是介绍脚本病毒，所以对 WSH 的功能不再作深入的介绍，有兴趣的读者可以参看相关的技术资料。



图 6-20　一个 WSH 的应用实例

4. WSH 的安全隐患及防治

任何事物都存在其两面性。WSH 在充分利用脚本来提高系统效率的同时，也增添了一些安全隐患。目前，大量的基于 WSH 的病毒在网络中泛滥，其中曾名躁一时的 I Love You 便是一个典型代表。因为 WSH 对多数用户来说基本上是没有用的，所以可以让 Windows 操作系统禁用 WSH 来达到对系统的安全保护。

在 Windows 操作系统中禁用 WSH 一般不会引起 IE 浏览器和系统的不正常，但在禁用了 WSH 后，一些需要 WSH 支持的软件将无法正常运行，用户也无法正常使用脚本来提高系统的运行效率。为此，用户在确认系统中不需要 WSH 的支持（目前大部分软件不需要

WSH 的支持)后,可以通过以下方法来禁用 WSH。

对于 Windows 2000/XP/2003 操作系统,首先打开“我的电脑”窗口,然后选择“工具”→“文件夹选项”命令,并在打开的“文件夹选项”对话框中选择“文件类型”选项卡,将打开如图 6-21 所示的对话框。其中,删除 VBS、VBE、JS 和 JSE 这 4 个扩展名的文件类型即可。之后,Windows 操作系统将完全无法运行脚本程序,所以从根本上预防了脚本病毒的入侵。



图 6-21 删除 VBS、VBE、JS 和 JSE 这 4 个扩展名的文件类型

6.4 木马的清除和防治方法

特洛伊木马(简称为“木马”,trojan)由于不感染其他的文件,也不破坏计算机系统,同时也不进行自我复制,所以木马不具有传统计算机病毒的特征。由于目前市面上的杀病毒软件一般都直接支持对木马的查杀,所以大家习惯于将木马称为“木马病毒”。木马主要用来作为远程控制、窃取密码的工具,它是一个具有内外连接功能的后门程序。

6.4.1 木马的特征

一般的木马程序包括客户端和服务器端两个程序,其中客户端用于攻击者远程控制植入木马的计算机(即服务器端),而服务器端即是植入木马程序的远程计算机。当木马程序或带有木马的其他程序执行后,木马首先会在系统中潜伏下来,并修改系统的配置参数,每次启动系统时都能够实现木马程序的自动加载。有时,木马程序会修改某一类型文件的关联,从而使木马的潜伏变得更加容易,并不易被用户发现。如图 6-22 所示,运行木马的客户端和服务器端在工作方式上属于客户机/服务器模式,其中,客户端在本地主机执行,用来控制服务器端。而服务器端则在远程主机上执行,一旦执行成功该主机就中了木马,就可以成为一台服务器,可以被控制者进行远程管理。

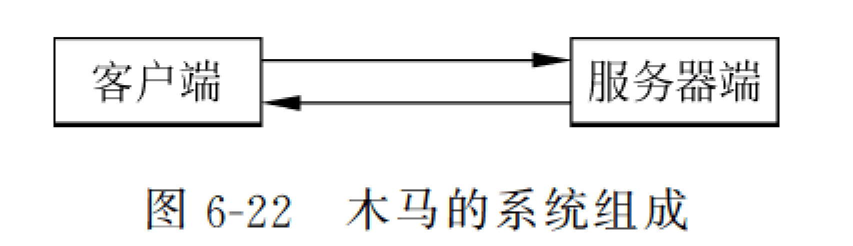


图 6-22 木马的系统组成

木马通常采取如图 6-23 所示的方式实施攻击：配置木马(伪装木马)→传播木马(通过文件下载或电子邮件等方式)→运行木马(自动安装并运行)→信息泄露→建立连接→远程控制。

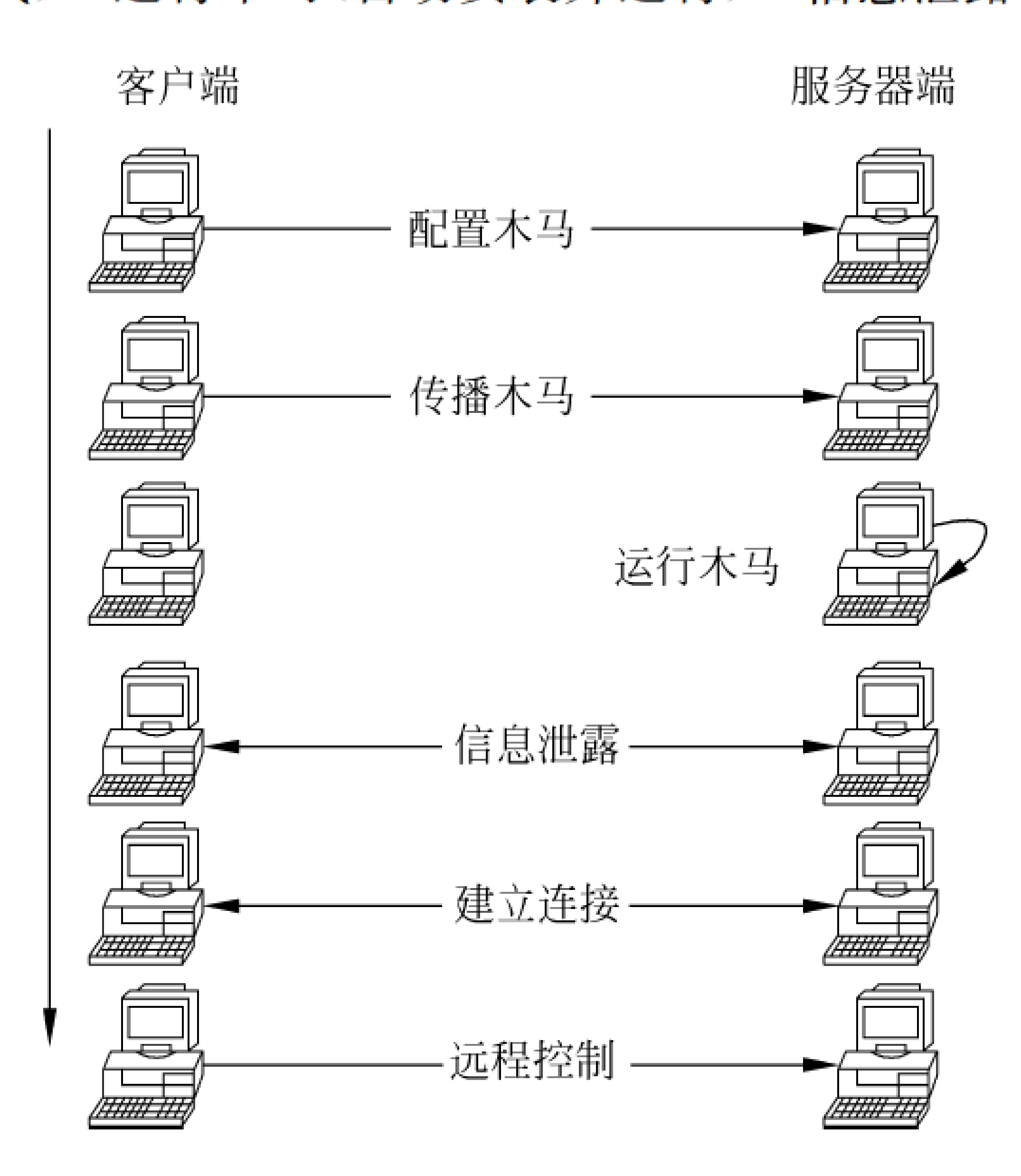


图 6-23　木马的运行过程

目前，木马入侵的主要途径是通过电子邮件的附件或文件下载等方式，将木马程序复制到用户的计算机中，然后通过修改系统配置文件或故意误导用户(如谎称有人给你送贺卡)使木马程序悄悄地在后台执行。一般的木马程序只有几 K 到几十 K 的大小，所以当木马程序隐藏在正常的文件中后用户一般很难发现。

木马也可以通过脚本、ActiveX 及 ASP. CGI 交互脚本的方式植入，由于 IE 浏览器在执行脚本时存在一些漏洞，这就为攻击者植入木马提供了便利。例如，曾出现过一个利用微软公司的 Scripts 脚本漏洞对用户的硬盘进行格式化的 HTML 页面。

6.4.2　木马的隐藏方式

由于木马所从事的是“地下工作”，因此为了防止“别人”发现它，它必须采取一定的方式隐藏起来。木马开发者一开始就想到了可能暴露木马踪迹的问题。例如木马会修改注册表和系统文件，以便计算机在下一次启动后仍能载入木马程序，而不需要生成一个启动程序。有些木马在服务器端实现了与正常程序的绑定，这种绑定称之为“exe-binder 绑定程序”，可以在使用被绑定的正常程序时实现木马的入侵。有些木马程序能把它自身的 exe 可执行文件和服务端的图片文件(如扩展名为. jpg、. bmp 的图片文件)绑定，在用户打开图片时，木马便侵入了系统。总体来看，木马主要通过以下几种方式进行隐藏。

1. 在“任务栏”里隐藏

这是木马最常采用的隐藏方式。为此，如果用户在 Windows 的“任务栏”里发现莫名其妙的图标，应怀疑可能是木马程序在运行。但现在的许多木马程序已实现了在任务栏中的隐藏，当木马运行时已不会在任务栏中显示其程序图标。

2. 在“任务管理器”里隐藏

在任务栏的空白位置单击鼠标右键，在弹出的快捷菜单中选择“任务管理器”命令，打开

其“进程”列表，就可以查看正在运行的进程。在进程列表中如果看到一些来路不明的名称，这时可以怀疑是木马程序。为了隐藏自己，现在的一些木马程序已实现了在进程中的伪装，使自己不出现在任务管理器里。有时，木马程序会将自己伪装为“系统服务”进程以骗过用户。

3. 隐藏通信方式

隐藏通信也是木马经常采用的手段之一。通过前面的介绍读者已经明白任何木马运行后都要和攻击者(客户端)进行通信连接。这种连接一般有直接连接和间接连接两种方式，其中“直接连接”是指攻击者通过客户端直接接入植有木马的主机(服务器端)；而“间接连接”即是如通过电子邮件、文件下载等方式，木马把侵入主机的敏感信息送给攻击者。现在大部分木马一般会在植入主机后，通过 TCP 或 UDP 端口进行驻留，而且有些木马多选择一些像 53、80 和 23 等常用的端口。例如，有一种木马还可以做到在通过 80 端口进行 HTTP 连接后，在收到正常的 HTTP 请求时仍然将其交给 Web 服务器进行处理，只有收到一些特殊约定的数据包时才调用木马程序。

4. 隐藏加载方式

木马在植入主机后如果不采取一定的方式运行也就等于在用户的计算机上存入了一个无用的文件，为此在木马值入主机后需要司机运行。在运行时，如果木马不做任何伪装会被用户很快发现，所以木马必须采取非常隐蔽的方式通过欺骗用户来运行。

木马为了控制服务端，必须在系统启动时跟随启动，所以它必须潜入用户计算机的启动配置文件中，如 win. ini、system. ini、winstart. bat 及启动组文件等。目前，随着一些互联网站的大量应用，为木马的植入和运行提供了方便之门，像 Java Script、VBScript、ActiveX 和 XML 等 WWW 的每一个新功能已几乎成为木马入侵的媒介。

5. 通过修改系统配置文件来隐藏

可以通过修改 VXD(虚拟设备驱动程序)或 DLL(动态链接库)文件来加载木马。这种方法与一般方法不同，它基本上摆脱了原有的木马所采用的监听端口进行连接的模式，而将木马程序改写成系统已知的 VXD 或 DLL 文件，以替代系统功能的方法来入侵。这样做的好处是没有增加新的文件，不需要打开新的端口，没有新的进程，使用常规的方法监测不到。在这种方式中，木马几乎没有表现出任何症状，且木马的控制端向被控制端发出特定的信息后，隐藏的程序就立即开始运行。

6. 具有多重备份功能

现在许多木马程序已实现了模块化，其中一些功能模块已不再由单一的文件组成，而是具有多重备份，可以相互恢复。当用户删除了其中的一个模块文件时，其他的备份文件就会立即运行。这类木马很难防治。

6.4.3 木马的种类

从木马程序产生以来，不但其隐蔽性得到加强，而且木马的编写和控制技术及功能也在不断加强。从总体来看，可以对目前已发现的木马程序进行以下的分类。

1. 远程控制型木马

远程控制型木马一般集成了其他木马和远程控制软件的功能，实现对远程主机的入侵和控制，包括访问系统的文件，截取主机用户的私人信息(包括系统账号、银行账号等)。在木马家族中，远程控制型木马是数量最多的一种，也是危害最大的一种，它可以让攻击者完

全控制已植入木马的主机,从事一些甚至连本地用户本身都不能顺利进行的操作。大家熟知的"冰河"就是一个远程控制型木马,当服务端程序运行时,客户端只要能够知道服务器的 IP 地址,就会方便地实现远程控制,从事像键盘记录、上传和下载信息、修改注册表等操作。

2. 密码发送型木马

密码发送型木马是专门为了窃取别人计算机上的密码而编写的,木马一旦被执行,就会自动搜索内存、Cache、临时文件夹及其他各种包含有密码的文件,如 Windows Server 2000、Windows Server 2003 的 SAM 文件中保存的 Administrator 账户密码等。一旦搜索到有用的密码,木马就会利用免费的电子邮件服务将密码发送到指定的邮箱,从而达到非法窃取别人计算机上密码的目的。这种木马的设计目的是找到所有的隐藏密码并且在用户不知道的情况下把密码发送到指定的信箱。

3. 键盘记录型木马

键盘记录型木马的设计目的主要是用于记录用户的键盘敲击,并且在日志文件(log 文件)中查找密码。该类木马分别记录用户在线和离线状态下敲击键盘时的按键信息。攻击者在获得这些按键信息后,很容易就会得到用户的密码等有用信息,包括用户可能在网上输入的银行账号。当然,在该类木马中,记录信息的返回一般也通过邮件发送功能来完成。

4. 破坏型木马

破坏型木马的功能比较单一,即破坏已植入木马的计算机上的文件系统,轻则使重要数据被删除,重则使系统崩溃。破坏型木马的功能与计算机病毒有些相似,不同的是破坏型木马的激活是由攻击者控制的,并且传播能力也比病毒慢。

5. DoS 攻击型木马

随着 DoS 和 DDoS(Distributed Denial of Service,分布式拒绝服务)攻击越来越广泛的应用,与之相伴的 DoS 攻击型木马也越来越流行。当黑客入侵了一台主机并植入了 DoS 攻击型木马,那么这台主机就成为黑客进行 DoS 攻击的最得力助手。黑客控制的主机越多,发起的 DoS 攻击也就越具有破坏性。由此可以看出,DoS 攻击型木马的危害不是体现在被植入木马的主机上,而是攻击者利用它作为攻击信息的发起源头来攻击其他的计算机,从而使被攻击的计算机瘫痪。

另外,还有一种称之为邮件炸弹的木马,它有些类似于 DoS 攻击型木马,一旦某台主机被植入并运行了木马,木马就会随机自动生成大量的邮件,并将其发送到特定的邮箱中,直到对方的邮件服务器瘫痪为止。

6. 代理型木马

在计算机网络中,代理是一种被广泛使用的技术。所谓代理其实就是一个跳板或中转,即两台主机之间的通信必须借助另一台主机(该主机在网络中称为代理服务器)来完成。代理型木马被植入主机后,像 DoS 攻击型木马一样,该主机本身不会遭到破坏。其实,代理型木马这样做的初衷便是掩盖自己的足迹,谨防别人发现自己的身份。通过代理型木马,攻击者可以在匿名的情况下使用 Telnet 远程登录程序及 ICQ、QQ 和 IRC 等即时信息程序,从而隐蔽自己的踪迹。

7. FTP 木马

FTP 木马使用了网上广泛使用的 FTP 功能，通过 FTP 使用的 TCP 21 端口来实现主机之间的连接。现在新型的 FTP 木马还加上了密码功能，这样只有攻击者本人才知道正确的密码，从而进入对方的计算机。FTP 木马是出现比较早的一类木马。

8. 程序杀手木马

程序杀手木马的功能就是关闭对方计算机上运行的某些程序（多为专门的防病毒或防木马程序），让其他的木马安全进入，实现对主机的攻击。

9. 反弹端口型木马

反弹端口型木马主要是针对防火墙而设计的。防火墙一般将网络分为内、外两部分，其中主要目的是保护内网资源。所以防火墙会对从外网进入内网的数据包进行严格的分析和过滤，而对从内网发往外网的数据包不作较多的处理。而木马的工作原理与防火墙正好相反，一般情况下，木马的攻击多由客户端发起，所以当被攻击者位于防火墙的内部时，位于外网的客户端将无法与位于内网的服务器端建立连接。

针对这类情况，便出现了反弹端口型木马。反弹端口型木马的服务端使用主动端口，客户端使用被动端口。木马定时监测控制端的存在，发现控制端可以连接后便立即弹出端口来主动连接控制端打开的主动端口。多数反弹端口型木马被动端口设置为 80 号端口，以避开用户使用端口扫描软件发现木马的存在。很显然，防火墙一般是不会封闭 80 号端口的，否则所有的 Web 页面将无法打开。

6.4.4 系统中植入木马后的症状

与计算机病毒一样，当木马入侵系统后也会表现出一定的症状。主要表现为以下几种。

1. 随意弹出窗口

虽然用户的计算机已经连接在网上，但并没有打开任何的浏览器。这时，如果系统突然弹出一个网上窗口，并打开某一个网站，这时有可能运行了木马。如果用户上网使用的是拨号方式，当系统突然进行自动拨号时，也可能是有木马在运行。

另外，在用户操作计算机时，有时会弹出一些警告框或信息提示对话框，这时也可能已运行了木马程序。

2. 系统配置参数发生改变

有的时候，用户使用的 Windows 操作系统的配置参数（如屏幕保护、时间和日期显示、声音控制、鼠标的形状及灵敏度、CD-ROM 的自动运行程序等）莫名其妙地被自动更改。

3. 频繁地读写硬盘

在计算机上并未进行任何操作时，如果系统频繁地读写硬盘（硬盘指示灯会不停地闪烁），有时软盘驱动器也会经常自己读盘，这时可能有木马在运行。

另外，在本章前面已经介绍过，木马还可能会在任务栏、任务管理器等处显示其运行的图标和进程。

6.4.5 木马的自运行方式

作为一个优秀的木马程序必须具备自启动功能，一个典型的例子就是把木马加入到用户经常执行的程序（如 explorer. exe、winword. exe）中，用户执行该程序时，木马则会自动运

行。木马更普遍的方法是通过修改 Windows 系统文件和注册表达到目的，主要表现在以下几个方面。

1. 在 win. ini 中启动

Windows 操作系统的 win. ini 文件，其中[windows]字段中有 load=和 run=两个启动命令，系统默认情况下这两条后面是空白的。如果木马要利用 win. ini 实现自运行，就可以将要运行的木马程序加载到这两条启动命令中。

2. 在 system. ini 中启动

在 Windows 的安装目录下有一个系统配置文件 system. ini，在[386Enh]字段下的"driver=路径\程序名"一般是木马经常加载的地方。而且，system. ini 中的[mic]、[drivers]和[drivers32]这三个字段主要是 Windows 操作系统来加载驱动程序，这也为添加木马程序提供了良好的场所。

3. 在 autoexec. bat 和 config. sys 中启动

在硬盘的第一个引导分区(一般为 C：分区)下存放着 autoexec. bat 和 config. sys 两个系统批处理和配置文件，这两个文件也是木马经常实现自运行的地方。

4. 在 Windows 启动组中启动

如果用户要在 Windows 操作系统启动时自动启动某一个程序，就可以将其添加到"开始"→"程序"→"启动"组中，所以 Windows 的启动组也成为木马经常选择的驻留之地。启动组对应的文件夹为 C:\Windows\start menu\programs\startup，在注册表中的位置为 HKEY_CURRENT_USER\Software\Microsoft\windows\CurrentVersion\Explorer\shell Folders 中的 Startup，如图 6-24 所示。

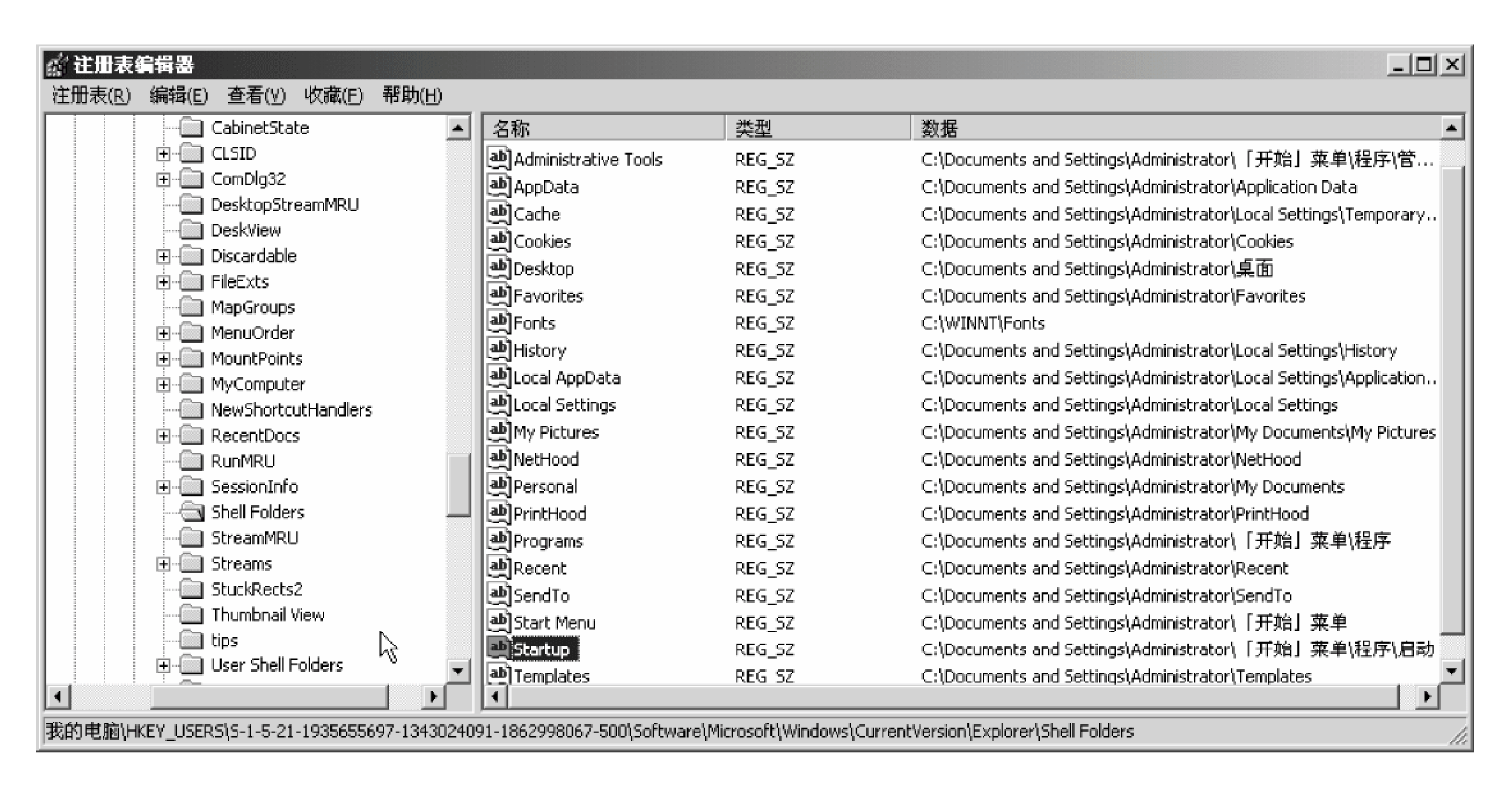


图 6-24 启动组在注册表中的位置

5. 修改文件关联

木马本身无法方便地实现自启动，就需要借助其他合法程序来完成，将这一过程称为文件关联。例如，在 Windows 下经常使用"记事本"工具(notepad. exe)来打开文本文件，但是如果被木马修改了 notepad. exe 的关联后，当打开. txt 的文本文件时，将会自动运行木马程

序。著名的国产木马"冰河"就是以这种方式实现木马程序的启动的。在修改了 notepad.exe 的文件关联后,一旦用户在打开.txt 文件时,就启动了木马程序。

6. 捆绑文件

当控制端和服务端已通过木马建立了连接后,控制端通过工具软件将木马文件和某一应用程序捆绑在一起后上传到服务端,并覆盖服务端的同名文件,这样当已运行的木马被发现并删除后,只要运行了捆绑有木马的应用程序,木马就会再次运行。现在,每一台上网的计算机一般都安装有杀病毒软件,而杀病毒软件一般在系统启动后都会自动运行,并驻留内存。所以,如果将木马程序捆绑到杀病毒程序后,那么每次 Windows 启动均会启动木马,而且杀病毒软件一般也不会发现该木马。

6.4.6 实验操作 4 木马的防治方法

防治木马的过程,其实就是预先采取一定的措施来预防木马进入系统,即将木马阻止在计算机之外的相关操作。

1. 防止以电子邮件方式植入木马

目前电子邮件的使用已非常广泛,每一个使用 Internet 的用户几乎都拥有自己的电子信箱。为此,大量的木马便利用电子邮件来植入用户的计算机系统。

木马在电子邮件中的位置一般有两种:附件和正文。早期的电子邮件正文多使用文本,很显然在文本中是无法隐藏木马程序的,所以木马只能藏匿在电子邮件的附件中,而且还采取双后缀名方式。一旦用户打开了藏有木马的附件,就将木马植入到了系统中。为预防这类木马,建议用户不要随意打开来路不明的电子邮件的附件。如果确实要打开不确定来历的电子邮件附件时,建议先将其下载到指定的文件夹中,用杀病毒软件查杀病毒并用专用查杀木马工具扫描后再打开。

现在的电子邮件系统在正文中已直接支持图片、HTML 页面等内容的显示,有些电子邮件系统还支持语音和视频。例如,当邮件正文中显示了 HTML 页面,并显示了一些链接时,一般不要单击这些链接。另外,HTML 页面中本身也可以隐藏不安全的代码,一旦打开这类邮件,不知不觉中就已感染了计算机病毒或植入了木马。对于利用邮件正文传播的病毒和木马,唯一可行的预防方法是不要打开这类邮件,而将其直接删除。

2. 防止在下载文件时植入木马

计算机网络的特点之一是提供了海量的信息和资源,其中包括一些软件。目前,很多网络用户已习惯于在网络上搜索和下载所需要的软件,但没有任何人能够保证网络上下载的软件是"干净"的。为了防止通过在网上下载文件时植入木马,建议服务器上安装的所有软件不要使用从网上下载的,对于客户机上使用的软件如果确实需要从网上下载的软件时,建议先将软件下载到某一个指定的文件夹中,用杀病毒软件查杀病毒并用专用查杀木马工具扫描后再安装使用。

建议习惯于从网上下载软件的用户使用专用的下载工具(如 FlashGet)来将文件下载到指定的文件夹中,同时把下载工具和杀病毒或查杀木马软件进行绑定,这样每当下载完一个文件后,下载工具便会利用已绑定的杀病毒或查杀木马软件对其进行自动扫描。以 FlashGet 为例,实现与杀病毒或查杀木马软件绑定的方法为:在 FlashGet 操作窗口中选择"工具"→"选项"→"文件管理"命令,在打开的如图 6-25 所示的"选项"对话框中选取"下载

完毕后进行病毒检查”复选框，并单击“浏览”按钮，选择本机上已使用的杀病毒或查杀木马软件名称，同时选择“下载完毕后打开或者查看已下载的文件”复选框。

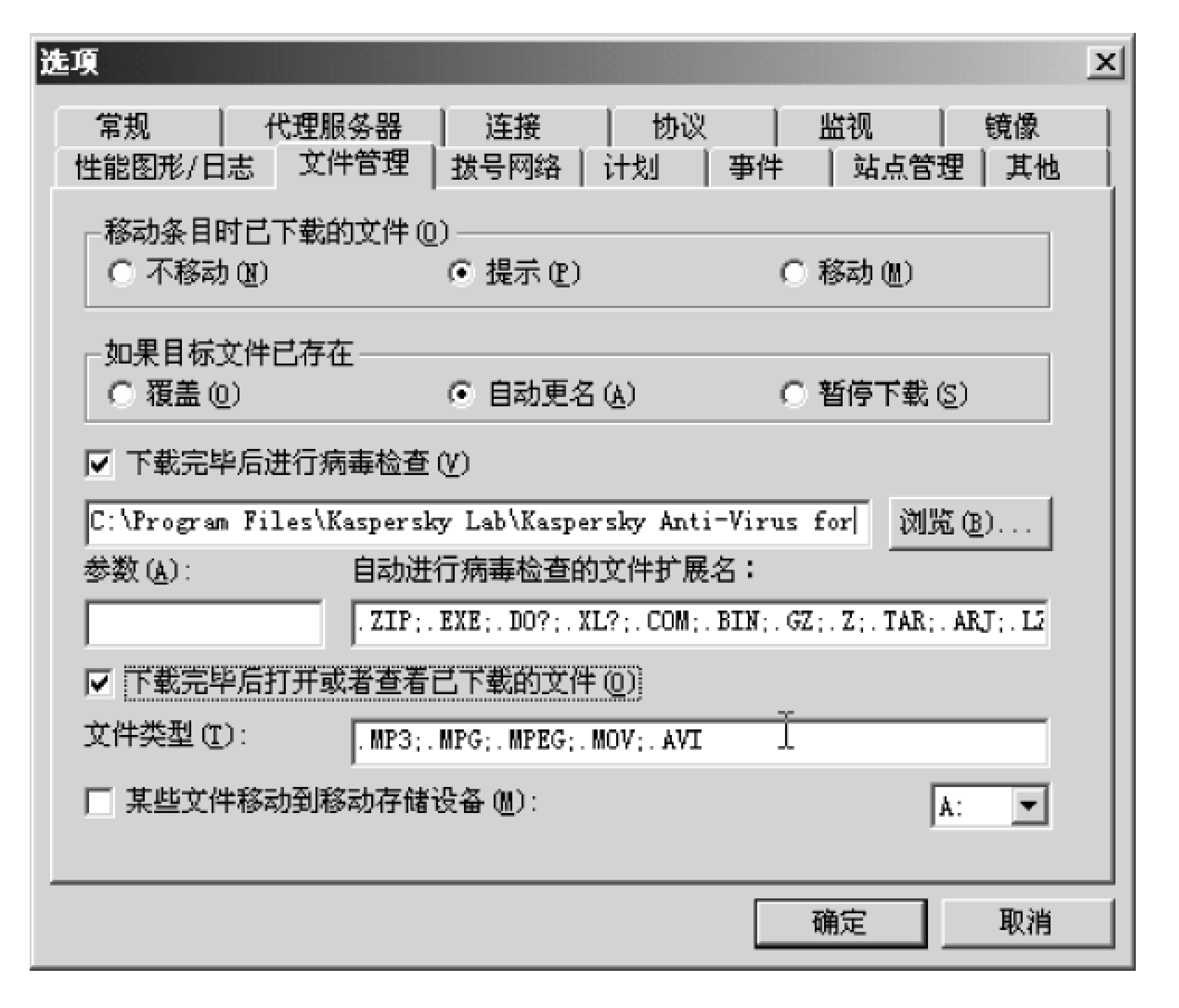


图 6-25　使用专用下载工具并绑定杀病毒软件

3. 防止在浏览网页时植入木马

由于 IE 浏览器本身存在的缺陷，许多程序可以在用户不知情的情况下安装在系统中，这也为木马的植入提供了一条途径。加强 IE 的安全性，一方面是使用最新版本的 IE 软件，因为新版本的 IE 修改了旧版本的许多不足，尤其在安全性方面得到了提高。同时，在使用任何一个 IE 时，都要及时升级 Services Pack 补丁程序，以修补 IE 存在的漏洞。另一方面是设置 IE 的设置属性，具体方法是在 IE 窗口中，选择“工具”→“Internet 选项”→“安全”命令，打开如图 6-26 所示的“Internet 选项”对话框。选取安全设置对象栏中的 Internet 后，单击“自定义级别”按钮。在打开的如图 6-27 所示的“安全设置”对话框中把“ActiveX 控件和插件”下的选项全部设置为“禁用”，这样就阻止了 IE 自动下载和执行文件的可能性。



图 6-26　“Internet 选项”对话框

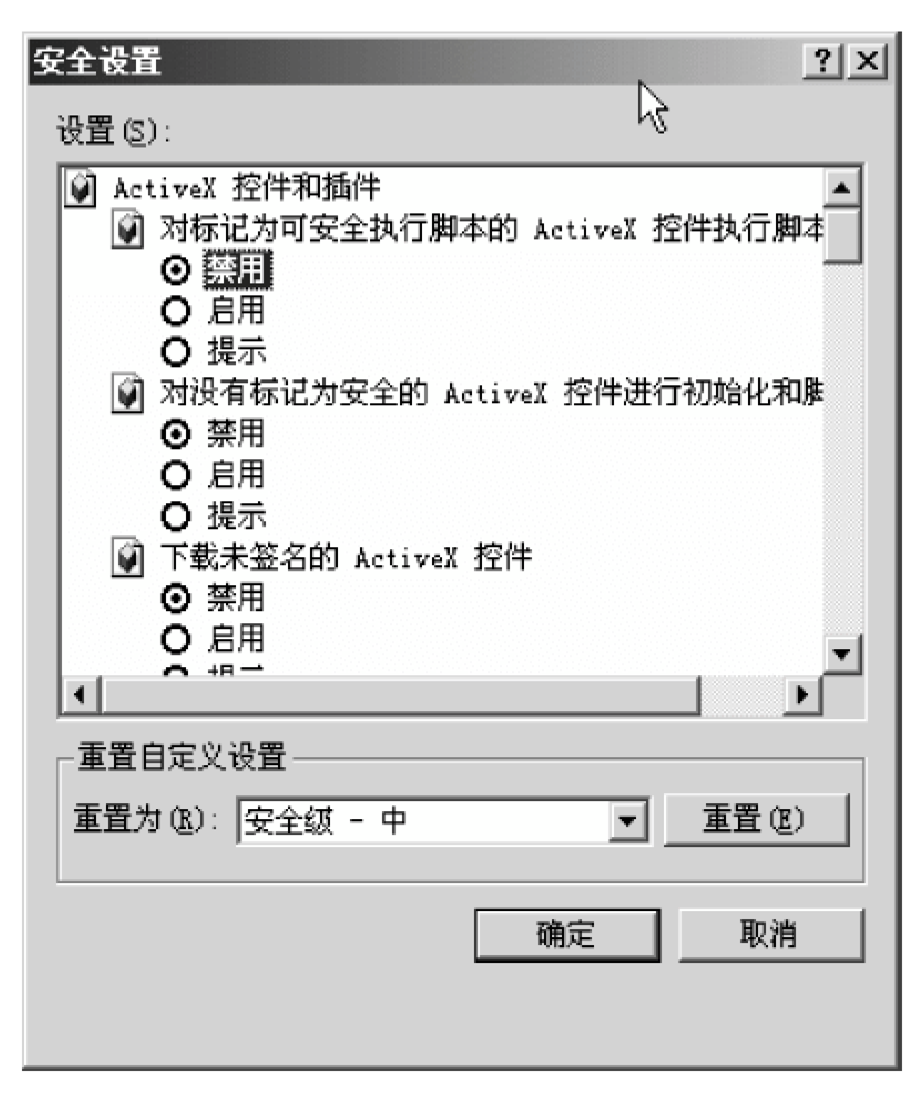


图 6-27　禁用 AcitveX 控件和插件

除此之外，还可以使用木马消除工具(如木马克星、木马分析专家和木马专家等)定期对计算机系统进行扫描。

6.5 间谍软件及防治方法

间谍软件是目前计算机网络中继病毒、蠕虫和木马之后新出现的一种以窃取他人信息和进行广告宣传为主的程序，已成为网络安全的重要隐患之一。

6.5.1 间谍软件的概念

间谍软件(Spyware)是一种能够在计算机用户不知情或没有感觉存在安全隐患的情况下，在用户的计算机上安装的“后门程序”软件。与计算机病毒不同的是，计算机上在运行了间谍软件后，对使用者来说并没有感觉到有什么异常，但用户的数据和重要信息可能会被间谍软件获取，并被发送到另一端的操纵者，甚至这些“后门程序”还能使黑客操纵用户的计算机。目前大家对间谍软件没有一个确切的定义，但间谍软件一般具有以下三大特征。

(1) 能够在用户不知情的情况下，将用户个人计算机的识别信息发送到因特网的某处，这些信息中也可能包括一些敏感的个人隐私信息。

(2) 没有病毒的传染性，同时不像病毒隐藏那么深，更不会感染文件。

(3) 能监视用户在网络上进行的一些操作、活动等，甚至访问了哪些网站都能监视到。

目前无论从技术还是从法律的角度，对间谍软件的界定还比较模糊。间谍软件最早被一些广告商用于监视和收集用户的网上行为、兴趣爱好和一些习惯性操作，他们将这些信息收集整理后转换为经济利益。而如今，间谍软件已被更多的公司及个人利用，其目的也从初期单纯地收集有用信息转化为今天的窃取他人信息，甚至直接盗取用户银行账号、密码。有些间谍软件还可以记录用户的键盘操作，捕捉并传送屏幕图像，具备一些木马程序的功能。

与间谍软件类似的有“广告软件”，该类软件只是能给某些特定的网站做宣传，自动弹出一些用户并不想访问的网站。目前将“广告软件”也归为“间谍软件”的范围。

目前对付间谍软件还没有十分有效的防治办法，国内反病毒厂商会将一些危害特征明显的间谍软件加入杀毒软件病毒库，而大部分“良性间谍软件”并没有被当作病毒查杀。国外一些安全厂商推出了反间谍软件(Anti-Spyware)程序，如 Ad-aware、SpyBot Search & Destroy 和 Windows AntiSpyware 等，但这些反间谍软件只能在一定程度上对已知间谍程序进行查杀。

6.5.2 间谍软件的入侵方式

在系统入侵方面，间谍软件在许多方面与木马有些类似。但由于间谍软件的出现相对较晚，所以在采取的技术上又表现出了一些特点。总体来看，间谍软件通过以下几种方式入侵用户的计算机系统。

(1) 捆绑。间谍软件或广告软件与另一个程序捆绑在一起，用户从表面上看到的是熟悉的系统或应用程序，但在该程序上却捆绑了间谍软件。

(2) 通过网页随机入侵。因特网上的许多提供免费下载的网站已成为间谍软件藏匿的场所。每当用户访问这些网站尤其是下载文件时，间谍软件就会乘机而入。

(3) 假冒实用程序。间谍软件会伪装成为一些实用程序而伺机入侵。例如,当用户从网上打开一个图片文件时,系统提示用户在浏览图片文件之前必须安装所需的浏览工具,这时一旦用户安装了所谓的“浏览工具”,间谍软件也就进入到用户的计算机系统。

通过以上几种主要的方式,间谍软件就可以进入用户的计算机系统。如果是一个广告软件,则会显示一些广告页面,或强迫浏览器进入到相关网站,或重新把用户引向由广告商控制的搜索结果,而不是显示用户习惯使用的搜索结果(如 Google、百度等)。

6.5.3 实验操作 5 反间谍工具 Spybot-Search & Destroy 的应用

Spybot-Search & Destroy(以下简称为 Spybot)是一款免费的反间谍软件,也是目前应用效果比较好的一款反间谍软件工具,同时它还支持中文操作(需要在安装时选择 Chinese (PRC),如图 6-28 所示),可运行在 Windows 9x/NT/2000/XP/2003 操作系统上。到目前为止,Spybot 已经可以检测出一万多种间谍程序,并可对其中的一千多种进行免疫处理。另外,当首次运行 Spybot 时,出于安全考虑系统建议备份当前计算机的注册表文件,如图 6-29 所示。

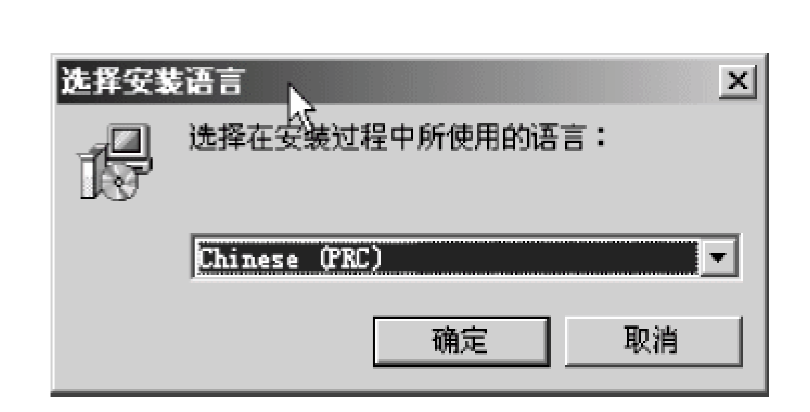


图 6-28 选择 Chinese(PRC)安装简体中文环境

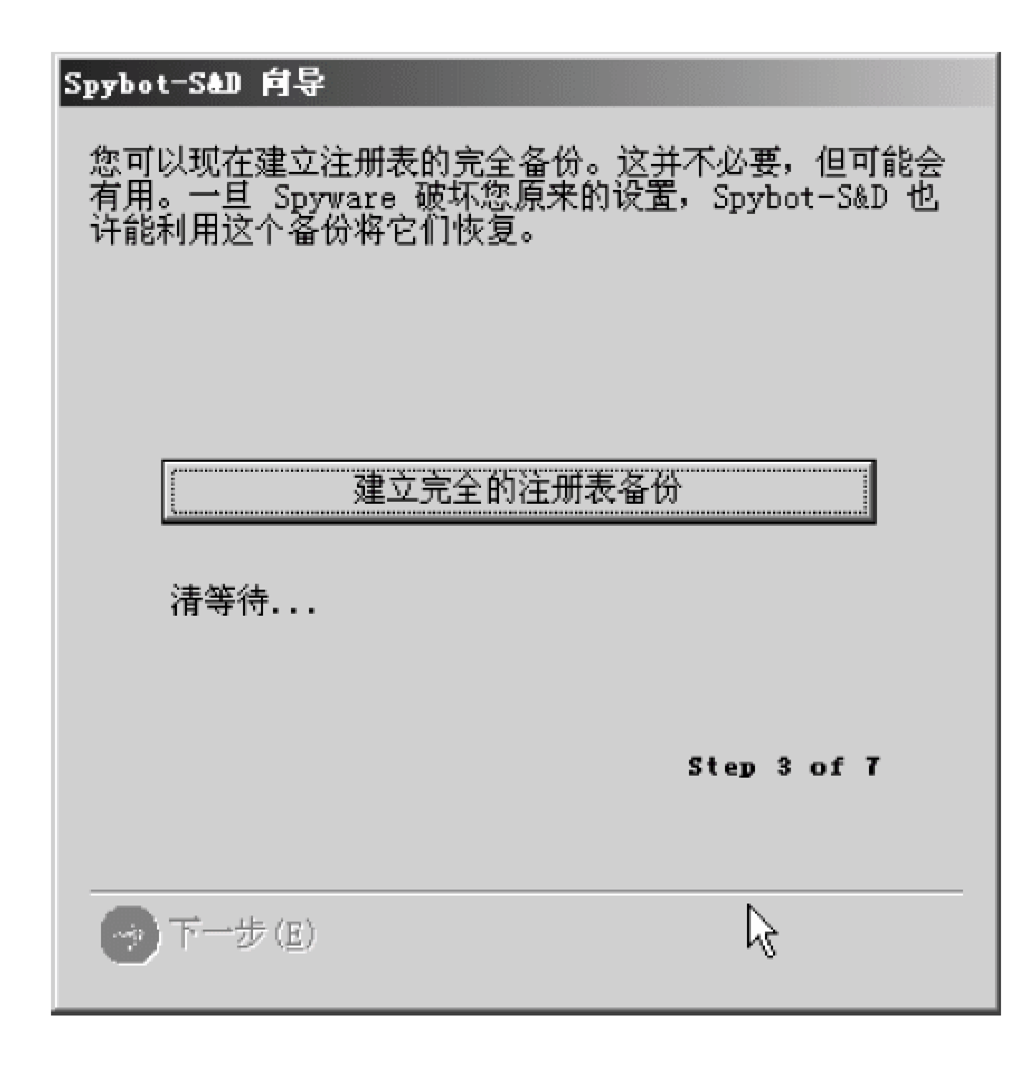


图 6-29 进行注册表的备份

1. 进行在线更新

Spybot 的操作主窗口如图 6-30 所示。需要说明的是,在使用 Spybot 之前必须通过网络对其进行在线数据库的更新。具体方法是:单击主窗口左边列表中的“更新”图标,在打开的对话框中单击“查找更新”按钮,在确保计算机已连接网络的情况下,Spybot 会通过网络下载要更新的内容,并显示在“更新”列表框中。在列表框中选取要更新的内容,然后单击“下载更新”按钮,系统开始下载所选择的更新内容,如图 6-31 所示。

2. 检查并清除间谍软件

单击主窗口左侧菜单上的“检查 & 清除”按钮,在打开的窗口中单击“检查问题”按钮,Spybot 开始检查当前计算机系统。根据计算机的配置及运行的软件情况,整个检查过程大概需要十几分钟,用户可以在主界面的状态栏上看到估计剩余的时间。检查结束后,便会列出查到的可能有问题的软件,如图 6-32 所示。



图 6-30　Spybot 操作主窗口



图 6-31　进行在线更新操作

选取某个已检查到的问题，然后单击右侧的显示详细信息按钮，可以查询到有关该问题软件的发布公司、软件功能、说明和危害种类等信息，如图 6-33 所示。

如果要修复某一问题，可先在如图 6-32 所示的列表框中选取要进行修复的软件名称，然后单击“修复”按钮，Spybot 便会自动为用户清除系统中的间谍软件，修复后的结果显示如图 6-34 所示。

3. 还原

经常使用各类杀病毒软件的用户可能总有这种经历：当清除了某种病毒后却发现某些软件无法运行了。如果用户在使用 Spybot 的“检查 & 清除”功能“修复”了已发现问题的软件后，却发现该软件无法运行了。这时，便可以使用“还原”功能来撤销前面的“修复”操作。



图 6-32　显示检测结果



图 6-33　显示某一软件的相关信息

具体操作方法是：单击主窗口左侧菜单中的“还原”按钮，在打开的如图 6-35 所示的对话框的“备份”列表中选取要还原的软件名称，然后单击“还原”按钮即可。

需要注意的是，当用户确信某个备份不需要时，建议删除这个备份以减少空间的占用。具体方法是：在图 6-35 所示的“备份”列表框中选取要删除的备份软件名称，然后单击“删除”按钮即可。

4. 免疫

Spybot 可以对 1000 多种间谍软件进行免疫处理。它通过对这些间谍软件的预防性处理，可有效地避免遭受这些间谍软件的危害。具体方法是：单击主窗口左侧列表框中的“免疫”按钮，Spybot 将自动检测当前计算机的免疫情况，并打开如图 6-36 所示的窗口，提示已



图 6-34　显示已修复的内容



图 6-35　还原已清除的软件

进行了免疫处理的有害软件的个数，显示当前有“0 个有害项目已免疫”，即还未进行免疫处理。要进行永久性免疫，可单击“免疫”按钮，Spybot 便会自动对系统进行免疫操作，结果如图 6-37 所示。同时，建议用户选取“允许在 IE 浏览器中永久封锁有害的网址”复选框，以实现双层保护的效果。

5．其他功能

如图 6-38 所示，在“工具”列表中，Spybot 还提供系统报告、文件粉碎机和后台监控等多种功能，用户可根据实际需要选择使用。例如，单击“IE 工具”按钮将打开如图 6-39 所示的窗口，在该窗口中可以对浏览器和系统的一些特性进行安全设置。



图 6-36　未进行免疫处理之前的显示信息



图 6-37　进行了免疫处理后的显示信息

6.5.4　实验操作 6　间谍软件的防治

间谍软件与计算机病毒不同，由于它一般不影响计算机的正常运行，所以当间谍软件入侵计算机系统后没有明显的症状。但事实上，凡是接入因特网的计算机基本上都有间谍软件在运行，所以对间谍软件进行防治是很有必要的。

Spybot 的首创人 Patrick Kolla 曾说过：“间谍软件制造者们正在系统中寻找新的、隐蔽性更强的地方来达到他们的目的，对于任何反间谍软件来说，挑战在于同时升级探测机制和探测数据库。”所以间谍软件与反间谍软件之间的较量将是一个长期的过程，在此过程中



图 6-38　Spybot 提供的其他工具



图 6-39　IE 工具设置

间谍软件是主导者，而反间谍软件总处于一种被动状态，像前面介绍的 Spybot 也只能在一定程度上对已知间谍程序进行查杀。因此，有效地防止已知和未知的间谍软件侵害将显得更为重要。以下是几种常用的防治方法。

1. 用好反间谍软件

像前面介绍的 Spybot 反间谍软件，通过用户设置可以定期进行扫描并发现系统中隐藏的间谍软件，对发现的可疑软件可以进行隔离、删除等操作，这在一定程度上保护了计算机系统。另外，如果要从源头开始防止间谍软件的入侵，可以选择安全性较高的操作系统，单机版建议使用 Windows XP SP2 及以上版本的操作系统，服务器版建议使用 UNIX/Linux

操作系统，也可以考虑使用 Windows Server 2003 或 2008 操作系统。相对于以前的操作系统，这些操作系统的安全性得到了较大的提高。例如，Windows XP SP2 和 Windows Server 2003 可以屏蔽网站的弹出窗口，因为不少间谍软件就是隐藏在网站的弹出窗口中而伺机进入用户的计算机系统的。另外，除选择使用一款较好的反间谍软件外，还要配置防火墙和杀病毒软件。其实，现在许多防火墙和杀病毒软件都提供了反间谍软件功能。

2. 尽量少使用 P2P 下载文件

P2P 的传统解释为 Peer-to-peer，即点对点通信。现在，P2P 已赋予了更广泛的应用，被称之为 Pointer-to-Pointer，即 PC-to-PC(计算机到计算机)。简单地说，P2P 就是指数据的传输不再通过服务器，而是在网络用户之间直接传递数据。由于 P2P 软件的特点，现在在因特网上的应用非常广泛，如 BT、电驴等。由于 P2P 软件的工作特点，致使两个利用 P2P 软件进行通信的计算机之间没有确定性，随之也就没有安全保护。正因为这样，现在因特网上的大量间谍软件被伪装成其他的可能引起用户关注的文件名，而等用户下载了这些软件后却被安装了间谍软件。

3. 关闭邮件的预览功能

现在的电子邮件正文一般都直接支持 HTML 页面，而 HTML 页面文件可以直接插入脚本等语言。这样，当用户打开被感染的 HTML 电子邮件的时候，间谍软件将被激活。所以，建议用户不要打开可疑邮件，同时关闭邮件收发软件的预览功能，这样可以在不打开的情况下就直接删除信息。以 Outlook 2003 为例，选择“工具”→“选项”命令，在打开的如图 6-40 所示的“选项”对话框中选取“阻止 HTML 电子邮件中的图像和其他外部内容”复选框。

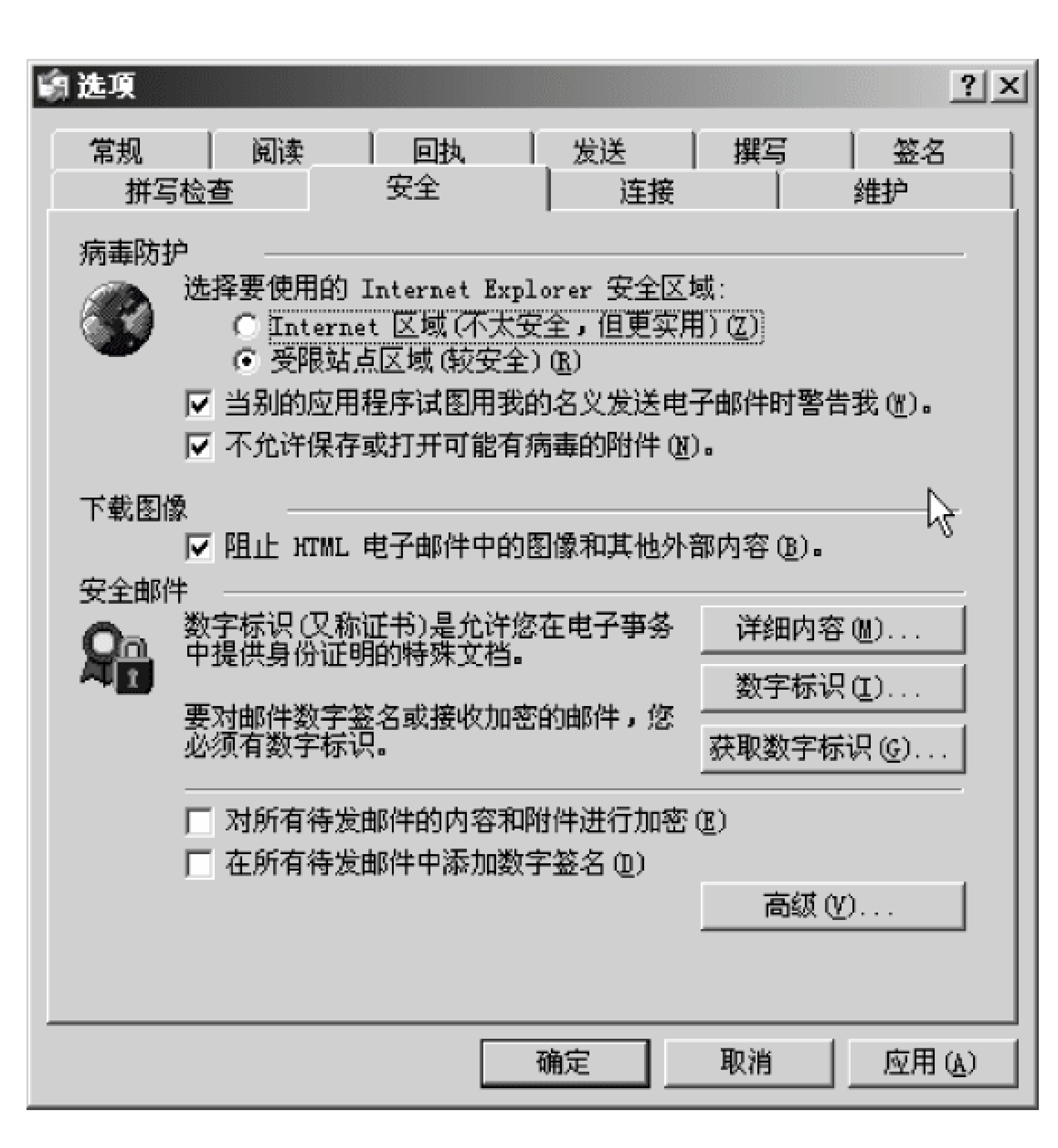


图 6-40 关闭对 HTML 中图片和其他内容的自动打开功能

4. 防止安装软件时安装间谍软件

我们在安装一些软件时系统会提示(有时根本不提示)同时安装其他的一些软件，有时被同时安装的这些软件就是间谍软件。为此，在安装软件之前或安装过程中，用户一定要仔

细阅读终端用户许可协议(End User License Agreements,EULA),因为有些 EULA 会告诉你如果安装了本软件,也就同时决定安装这个软件中带有的间谍软件。

另外,在 IE 浏览器中,应将安全设置至少处于中等水平,同时禁止浏览器安装任何用户没有要求的 ActiveX 控制件。

习　　题

6-1　名词解释:计算机病毒、多态病毒、蠕虫、木马。
6-2　计算机病毒具有哪些特征?
6-3　目前流行的计算机病毒可分为哪几类? 分别具有哪些特点?
6-4　计算机病毒与蠕虫和木马有哪些区别?
6-5　计算机在感染了蠕虫后有哪些具体的表现形式?
6-6　如何防治蠕虫病毒?
6-7　什么是脚本? 常用的脚本软件有哪些?
6-8　如何防治脚本病毒?
6-9　与蠕虫和脚本病毒相比,木马有哪些具体的特征?
6-10　如何判断系统中被植入了木马程序?
6-11　如何防治木马?
6-12　什么是间谍软件? 间谍软件对系统有哪些危害?
6-13　如何清除和防治间谍软件?

第7章　网络攻击与防范

因特网的无处不在和无所不能已经完全改变了人们对“网络”这个概念已有的定义。20世纪70年代以前，计算机网络还基本上是完全孤立存在。而现在这种无处不在的网络在能够使用户完成过去不可想象的工作的同时，也为各类网络入侵、攻击甚至是犯罪提供了平台。为了应付各种威胁，用户开始应用入侵检测系统(IDS)，通过IDS来监视经过网络和服务器的通信。针对IDS存在的不足，IPS则从防御入手对网络进行安全防护。本章在重点介绍各类网络攻击手段后，将有针对性地介绍DoS/DDoS、IDS、IPS的工作原理和防范方法。需要说明的是，由于各类安全产品操作方法的差异性，本章不再具体就某一种产品介绍其应用，而是着重介绍相关的技术特点及应用功能，以此培养读者选择和部署网络安全产品的能力。

7.1　网络攻击概述

随着网络应用的日渐普及，安全威胁日显突出，其中网络攻击成为目前网络安全中危害最严重的现象之一，所以研究和解决各种攻击方法将显得很有必要。

7.1.1　网络入侵与攻击的概念

网络入侵是一个广义上的概念，它是指任何威胁和破坏计算机或网络系统资源的行为，例如非授权访问或越权访问系统资源、搭线窃听网络信息等。具有入侵行为的人或主机称为入侵者。一个完整的入侵包括入侵准备、攻击和侵入实施等过程。而攻击是入侵者进行入侵所采取的技术手段和方法，入侵的整个过程都伴随着攻击，有时也把入侵者称为攻击者。

其实，在整个网络行为中，入侵和攻击仅仅是在形式和概念描述上有所不同，其实质基本上是相同的。对计算机和网络系统而言，入侵与攻击没有本质的区别，入侵伴随着攻击，攻击的结果就是入侵。例如，在入侵者没有侵入目标网络之前，会采取一些方法或手段对目标网络进行攻击。当攻击者侵入目标网络之后，入侵者利用各种手段窃取和破坏别人的资源。

从网络安全角度看，入侵和攻击的结果都是一样的。一般情况下，入侵者或攻击者可能是黑客、破坏者、间谍、内部人员、被雇用者、计算机犯罪者或恐怖主义者。攻击时，所使用的工具(或方法)可能是电磁泄漏、搭线窃听、程序或脚本、软件工具包、自治主体(能独立工作的小软件)、分布式工具、用户命令或特殊操作等。在本章的描述中，将集中使用攻击这一概念。

入侵者(或攻击者)所采用的攻击手段主要有以下 8 种特定类型。

(1) 冒充。将自己伪装成为合法用户(如系统管理员),并以合法的形式攻击系统。

(2) 重放。攻击者首先复制合法用户所发出的数据(或部分数据),然后进行重发,以欺骗接收者,进而达到非授权入侵的目的。

(3) 篡改。通过采取秘密方式篡改合法用户所传送数据的内容,实现非授权入侵的目的。

(4) 拒绝服务。中止或干扰服务器为合法用户提供服务或抑制所有流向某一特定目标的数据。

(5) 内部攻击。利用其所拥有的权限对系统进行破坏活动。这是最危险的类型,据有关资料统计,80%以上的网络攻击及破坏与内部攻击有关。

(6) 外部攻击。通过搭线窃听、截获辐射信号、冒充系统管理人员或授权用户、设置旁路躲避鉴别和访问控制机制等各种手段入侵系统。

(7) 陷阱门。首先通过某种方式侵入系统,然后安装陷阱门(如值入木马程序)。并通过更改系统功能属性和相关参数,使入侵者在非授权情况下能对系统进行各种非法操作。

(8) 特洛伊木马。这是一种具有双重功能的客户/服务体系结构。特洛伊木马系统不但拥有授权功能,而且还拥有非授权功能,一旦建立这样的体系,整个系统便被占领。

7.1.2 拒绝服务攻击

拒绝服务攻击是出现较早、实施较为简单的一种攻击方法。它是攻击者利用一定的手段,让被攻击主机无法响应正常的用户请求。拒绝服务攻击主要表现为以下几个方面。

1. 死亡之 ping

死亡之 ping(ping of death)是最常使用的拒绝服务攻击手段之一,它利用 ping(Packet Internet Groper)命令发送不合法长度的测试包来使被攻击者无法正常工作。在早期的网络中,路由器对数据包的最大尺寸都有限制,在 TCP/IP 网络中,许多系统对 ICMP 包的大小都规定为 64KB。当 ICMP 包的大小超过该值时就导致内存分配错误,直致 TCP/IP 协议栈崩溃,最终使被攻击主机无法正常工作。

在基于 TCP/IP 协议的 Internet 广泛使用的今天,为了阻止死亡之 Ping,现在所使用的网络设备(如交换机、路由器和防火墙等)和操作系统(如 UNIX、Linux、Windows 和 Solaris 等)都能够过滤掉超大的 ICMP 包。以 Windows 操作系统来说,单机版从 Windows 98 之后,Windows NT 从 Service Pack 3 之后都具有抵抗一般 ping of death 攻击的能力。

2. 泪滴

在 TCP/IP 网络中,不同的网络对数据包的大小有不同的大小规定,例如以太网的数据包最大为 1500B(将数据包的最大值称为最大数据单元,MTU),令牌总线网络的 MTU 为 8182B,而令牌环网和 FDDI 对数据包没有大小限制。如果令牌总线网络中一个大小为 8000B 的 IP 数据包要发送到以太网中,由于令牌总线网络的数据包要比以太网的大,所以为了能够完成数据的传输,需要根据以太网数据包的大小要求,将令牌总线网络的数据包分成至少 6 部分(1500×6=9000),将这一过程称为分片。

在 IP 报头中有一个偏移字段和一个分片标志(MF),如果 MF 标志设置为 1,则表明这

个 IP 数据包是一个大 IP 数据包的片段,其中偏移字段指出了这个片段在整个 IP 数据包中的位置。例如,对一个 4500B 的 IP 数据包进行分片(MTU 为 1500),则三个片段中偏移字段的值依次为 0、1500、3000。这样接收端就可以根据这些信息成功地重组该 IP 数据包。

如果一个攻击者打破这种正常的分片和重组 IP 数据包的过程,把偏移字段设置成不正确的值(假如,把上面的偏移设置为 0、1300、3000),在重组 IP 数据包时可能会出现重合或断开的情况,就可能导致目标操作系统崩溃。这就是所谓的泪滴(teardrop)攻击。

防范泪滴攻击的有效方法是给操作系统安装最新的补丁程序,修补操作系统漏洞。同时,对防火墙进行合理地设置,在无法重组 IP 数据包时将其丢弃,而不进行转发。

3. ICMP 泛洪

ICMP 泛洪(ICMP flood)是利用 ICMP 报文进行攻击的一种方法。在平时的网络连通性测试中,经常使用 ping 命令来诊断网络的连接情况。如图 7-1 所示,当输入了一个 ping 命令后,就会发出 ICMP 响应请求报文(ICMP ECHO),接收主机在接收到 ICMP ECHO 后,会回应一个 ICMP ECHO Reply 报文(图 7-1 中共收回了 4 个 ICMP ECHO Reply 报文)。在这个过程中,当接收端收到 ICMP ECHO 报文进行处理时需要占用一定的 CPU 资源。如果攻击者向目标主机发送大量的 ICMP ECHO 报文,将产生 ICMP 泛洪,目标主机会将大量的时间和资源用于处理 ICMP ECHO 报文,而无法处理正常的请求或响应,从而实现对目标主机的攻击。

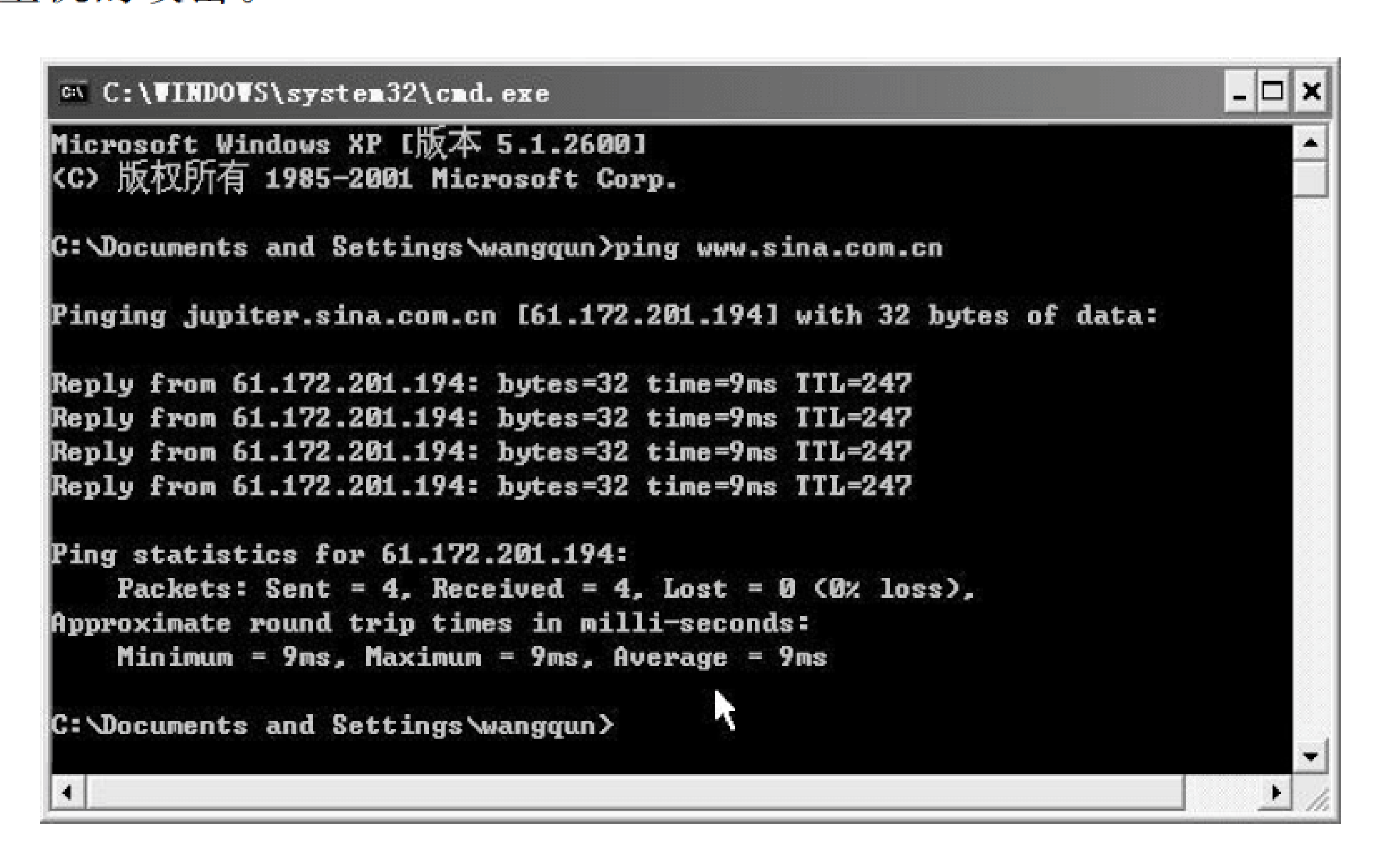


图 7-1　利用 ping 命令发出的 ICMP 报文来测试网络连接情况

防范 ICMP 泛洪的有效方法是对防火墙、路由器和交换机进行相应设置,过滤来自同一台主机的、连续的 ICMP 报文。对于网络管理员来说,在网络正常运行时建议关闭 ICMP 报文,即不允许使用 ping 命令。例如,如图 7-2 所示,在 Windows XP/2003 系统中启用了 Internet 连接防火墙后,则默认所有的 ICMP 报文选项均被禁用,从而可以阻止来自网络的 ping 试探。

4. UDP 泛洪

UDP 泛洪(UDP flood)的实现原理与 ICMP 泛洪类似,攻击者通过向目标主机发送大量的 UDP 报文,导致目标主机忙于处理这些 UDP 报文,而无法处理正常的报文请求或响应。

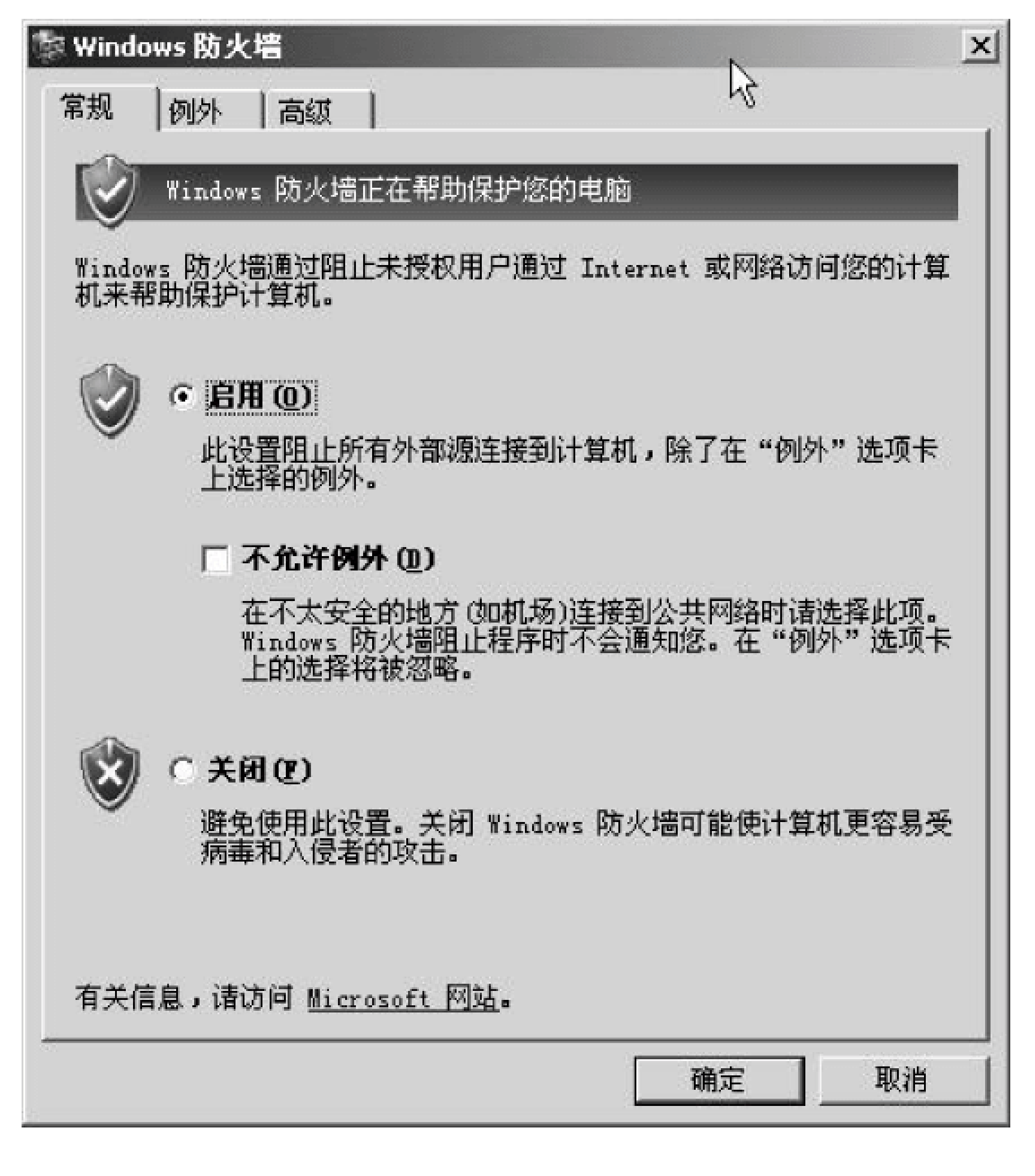


图 7-2　启用 Internet 防火墙

5. LAND 攻击

LAND 攻击利用了 TCP 连接建立的三次握手过程，通过向一个目标主机发送用于建立请求连接的 TCP SYN 报文而实现对目标主机的攻击。与正常的 TCP SYN 报文不同的是，LAND 攻击报文的源 IP 地址和目的 IP 地址是相同的，都是目标主机的 IP 地址。这样，目标主机在收到这个 SYN 报文后，就会向该报文的源地址发送一个 ACK 报文，并建立一个 TCP 连接控制结构，而该报文的源地址就是自己。由于目的 IP 地址和源 IP 地址是相同的，都是目标主机的 IP 地址，因此这个 ACK 报文就发给了目标主机本身。

利用该过程，当攻击者发送 SYN 报文达到一定的数量时，目标主机的连接控制结构将会被耗尽，从而无法为其他用户提供正常的服务。

防范 LAND 攻击的可行方法是给操作系统安装最新的补丁程序，同时在网络设备(如防火墙、路由器和交换机等)上进行相应的配置，将那些通过外部接口进入内部网络的含有内部源地址的 IP 数据包过滤掉。

6. Smurf 攻击

如图 7-1 所示，在网络连通性诊断中通常使用 ICMP ECHO，当一台主机接收到这样一个报文后，会向报文的源地址回应一个 ICMP ECHO REPLY 应答报文。在 TCP/IP 网络中，一般情况下主机不会检查该 ICMP ECHO 请求的源地址。利用该“漏洞”，攻击者可以把 ICMP ECHO 的源地址设置为一个广播地址或某一子网的 IP 地址，这样目标主机就会以广播形式回复 ICMP ECHO REPLY，导致网络中产生大量的广播报文，形成广播风暴。轻则影响网络的正常运行，重则由于耗用过量的网络带宽和主机(如路由器、交换机等)资源，导致网络瘫痪。将这种利用虚假源 IP 地址进行 ICMP 报文传输的攻击方法称为 Smurf 攻击。

为了防止 Smurf 攻击，在路由器、防火墙和交换机等网络硬件设备上可关闭广播、组播等特性。对于位于网络关键部位的防火墙，则可以关闭 ICMP 数据包的通过。

另外,还有借助 TCP 三次握手的拒绝服务,这部分内容读者参看本书第 5 章的相关章节。

7. 电子邮件炸弹

电子邮件炸弹(E-mail Bomb)是指电子邮件的发送者利用某些特殊的电子邮件软件,在很短时间内连续不断地将大容量的电子邮件发送给同一个收件人,而一般收件人的邮箱容量是有限的,同时电子邮件服务器也很难接收这些数以千万计的大容量信件,其结果是导致电子邮件服务器不堪重负,最终崩溃。

电子邮件炸弹是最古老、最简单的一种攻击方法,也是最有效的方法之一。当一台或多台计算机向某一台邮件服务器不断发送大容量的电子邮件时,轻则耗尽接收者的网络带宽,重则使邮件服务器瘫痪。防范电子邮件炸弹的有效方法是在邮件服务器或防火墙设备上进行相关的设置,使其自动删除来自同一台主机的过量或重复的邮件。

7.1.3 利用型攻击

利用型攻击是一类试图直接对用户的主机进行控制的攻击方法,最常见的有以下三种。

1. 口令攻击

口令(也称“密码”)是网络安全的第一道防线,但从目前的技术来看,口令已没有足够的安全性,各种针对口令的攻击不断出现。所谓口令攻击是指通过猜测或获取口令文件等方式获得系统认证口令,从而进入系统。目前,网络中存在的弱口令(也称为危险口令)主要有用户名、用户名的变形、生日、常用的英文单词、5 个字符以下长度的口令、空口令或系统默认的口令(如 Admin、manager 和 supervisor 等)。

攻击者在识别了一台主机,并且发现了基于 NetBIOS、Telnet 或 NFS 等服务的可利用的用户账号的口令时,便会实现对主机的控制。有效的防范方法是选用难以猜测的口令,关闭主机上不需要的 NFS、NetBIOS 和 Telnet 等服务。

2. 特洛伊木马

特洛伊木马是一个包含在合法程序中的非法程序。该非法程序在用户不知情的情况下被执行。特洛伊木马的名称源于古希腊的特洛伊木马神话,传说希腊人围攻特洛伊城,久久不能得手。后来想出了一个木马计,让士兵藏匿于巨大的木马中。大部队假装撤退而将木马摒弃于特洛伊城,让敌人将其作为战利品拖入城内。木马内的士兵则乘夜晚敌人庆祝胜利、放松警惕的时候从木马中爬出来,与城外的部队里应外合而攻下了特洛伊城。

一般的木马都有客户端和服务器端两个执行程序,其中客户端用于攻击者远程控制植入木马的机器,服务器端程序即木马程序。攻击者要通过木马攻击用户的系统,所做的第一步工作是要把木马的服务器端程序植入到用户的计算机中。有关特洛伊木马的相关知识已在本书第 6 章进行了详细介绍,在此不再赘述。

3. 缓冲区溢出

缓冲区溢出攻击利用了目标程序的缓冲区溢出漏洞,通过操作目标程序堆栈并暴力改写其返回地址,从而获得目标控制权。缓冲区溢出的工作原理是:攻击者向一个有限空间的缓冲区中复制过长的字符串,这时可能产生两种结果:一是过长的字符串覆盖了相邻的存储单元而造成程序瘫痪,甚至造成系统崩溃;二是可让攻击者运行恶意代码,执行任意指令,甚至获得管理员用户的权限等。

利用缓冲区溢出漏洞而发起的攻击非常普遍。例如，1988 年，美国康奈尔大学计算机科学系 23 岁的研究生莫里斯，他利用 UNIX fingered 程序不限制输入长度的漏洞，输入 512 个字符后使缓冲器溢出。莫里斯又写了一段特别大的程序使他的恶意程序能以 root(根)身份执行，并感染到其他机器上。另外，曾破坏过大量数据库系统的 SQL Slammer 蠕虫王，也是利用未及时更新补丁的 MS SQL Server 数据库缓冲区溢出漏洞，采用不正确的方式将数据发到 MS SQL Server 的监听端口，引起缓冲溢出攻击。

7.1.4 信息收集型攻击

与前面介绍的拒绝服务攻击不同，信息收集型攻击并不对目标主机本身造成危害，而是将目标主机作为一个跳板，用来对其他主机进行攻击。信息收集型攻击主要包括扫描技术、体系结构刺探和利用信息服务等类型。

1. 扫描技术

扫描技术主要分为两类：主机安全扫描技术和网络安全扫描技术，其中网络安全扫描技术主要针对系统中存在的弱口令或与安全规则相抵触的对象进行检查；而主机安全扫描技术则是通过执行一些脚本文件，对系统进行模拟攻击，同时记录系统的反应，从而发现其中的漏洞。常见的扫描技术主要有端口扫描和漏洞扫描。

1) 端口扫描技术

一个端口就是一个潜在的通信通道，也是一个入侵通道。对目标主机进行端口扫描，能得到许多有用的信息。根据 TCP 协议规范，当一台主机收到一个 TCP 连接建立请求报文(TCP SYN)时，需要做以下的工作：如果请求的 TCP 端口是开放的，则返回一个 TCP ACK 确认报文，并建立 TCP 连接控制结构(TCB)；如果请求的 TCP 端口没有开放，则返回一个 TCP RST(TCP 头部中的 RST 标志设为 1)报文，告诉 TCP 连接的发起端该端口没有开放。

与 TCP 相似，如果主机收到一个 UDP 报文，需要进行以下的工作：如果该报文的目标端口开放，则把该 UDP 报文上交给其上层协议进行处理，由于 UDP 为面向非连接的协议，所以它并不返回任何报文；如果该报文的目标端口没有开放，则向 UDP 信息的发送者返回一个 ICMP 不可到达的报文，告诉发送方该 UDP 报文的端口不可到达。

利用这个原理，攻击者便可以通过发送合适的报文来判断目标主机哪些 TCP 或 UDP 端口是开放的，过程如下。

① 发出 TCP SYN 或 UDP 报文，端口号从 0 开始，一直到 65535。

② 如果收到了针对这个 TCP 报文的 RST 报文，或针对这个 UDP 报文的 ICMP 不可到达的报文，则说明这个端口没有开放。

③ 如果收到了针对这个 TCP SYN 报文的 ACK 报文，或者没有接收到任何针对该 UDP 报文的 ICMP 报文，则说明该 TCP 或 UDP 端口可能是开放的。

通过以上操作，便可以很容易地判断出目标主机开放了哪些 TCP 或 UDP 端口，然后利用端口进行一下步的攻击。

2) 漏洞扫描技术

漏洞扫描主要通过以下两种方法来检查目标主机是否存在漏洞：在端口扫描后得知目标主机开启的端口及端口上的网络服务，将这些相关信息与网络漏洞扫描系统提供的漏洞

库进行匹配,查看是否有满足匹配条件的漏洞存在;通过模拟黑客的攻击手法,对目标主机系统进行攻击性的安全漏洞扫描,如测试弱口令等。如果模拟攻击成功,则表明目标主机系统存在安全漏洞。

2. 体系结构探测

体系结构探测,是指攻击者使用具有已知响应类型的数据库的自动工具,对来自目标主机的响应进行检查,从而探测到目标主机的操作系统、数据库的类型和版本等信息,为进一步入侵作好准备。例如,在 Windows 2000/2003 操作系统中对 TCP/IP 协议的实现与 Solaris 有所不同,所以每种操作系统都有其独特的响应方法。攻击者在获得独特的响应后,再与数据库中已知的响应进行对比,便可以确定出目标主机所运行的操作系统。

3. 利用信息服务

利用信息服务中最有代表性的是 finger 服务。finger 是计算机网络中最古老的协议之一,用于提供站点及用户的基本信息。利用 79 号端口,通过 finger 服务可以查询到网站上的在线用户清单及其他一些有用的信息。出于安全考虑,目前大部分网站取消了 finger 服务,不过还有部分主机仍然在继续提供 finger 服务。在 UNIX 平台上,finger 是一个常用的工具。

由于 finger 服务一般都是提供在线用户的用户名,因此入侵者通过 finger 服务可以方便地取得有效用户名列表,然后使用暴力破解等方法获得用户的账号、密码,为进一步入侵作好准备。

7.1.5 假消息攻击

假消息攻击主要包括 DNS 缓存中毒和伪造电子邮件两类。

1. DNS 缓存中毒

由于 DNS 服务器与其他名称服务器交换信息的时候并不进行身份验证,这就使得攻击者可以将不正确的信息加入其中并把用户引向攻击者自己的主机。

现代计算机网络尤其是 Internet 离不开 DNS 服务。为了提高 DNS 服务器的工作效率,绝大部分 DNS 服务器都能够将 DNS 查询结果在答复给发出请求的主机之前保存在高速缓存中。但是,如果 DNS 服务器的高速缓存中被大量假的 DNS 信息所“污染”,用户的请求就有可能被送到一些恶意或不健康的网站,而不是他们原本要访问的网站。

绝大部分 DNS 服务器都能够通过配置来阻止缓存中毒。基于 Windows Server 2003 的 DNS 服务器默认的配置状态就能够防止缓存污染。如果用户使用的是基于 Windows 2000 的 DNS 服务器,可以通过配置来防止缓存污染。具体方法是:选择“开始”→“程序”→“管理工具”→DNS,打开 DNS 服务器,选取 DNS 服务器名称后单击鼠标右键,在弹出的快捷菜单中选择“属性”命令,在打开的如图 7-3 所示的“SERVERI 属性”对话框中选取“服务器选项”列表框中的“保护缓存防止污染”复选项,然后重新启动 DNS 服务器即可。

有关 DNS 缓存中毒的详细介绍,读者可参看本书第 5 章的相关内容。

2. 伪造电子邮件

在发送电子邮件时,由于所使用的 SMTP 协议并不对邮件发送者的身份进行鉴别,因此攻击者便可以伪造并发送大量的电子邮件。这些电子邮件一般还会附上可安装的特洛伊木马程序,或者是一个引向恶意或不健康网站的链接。目前,Internet 中大量的垃圾邮件都是通过伪造电子邮件的方式来发送的。

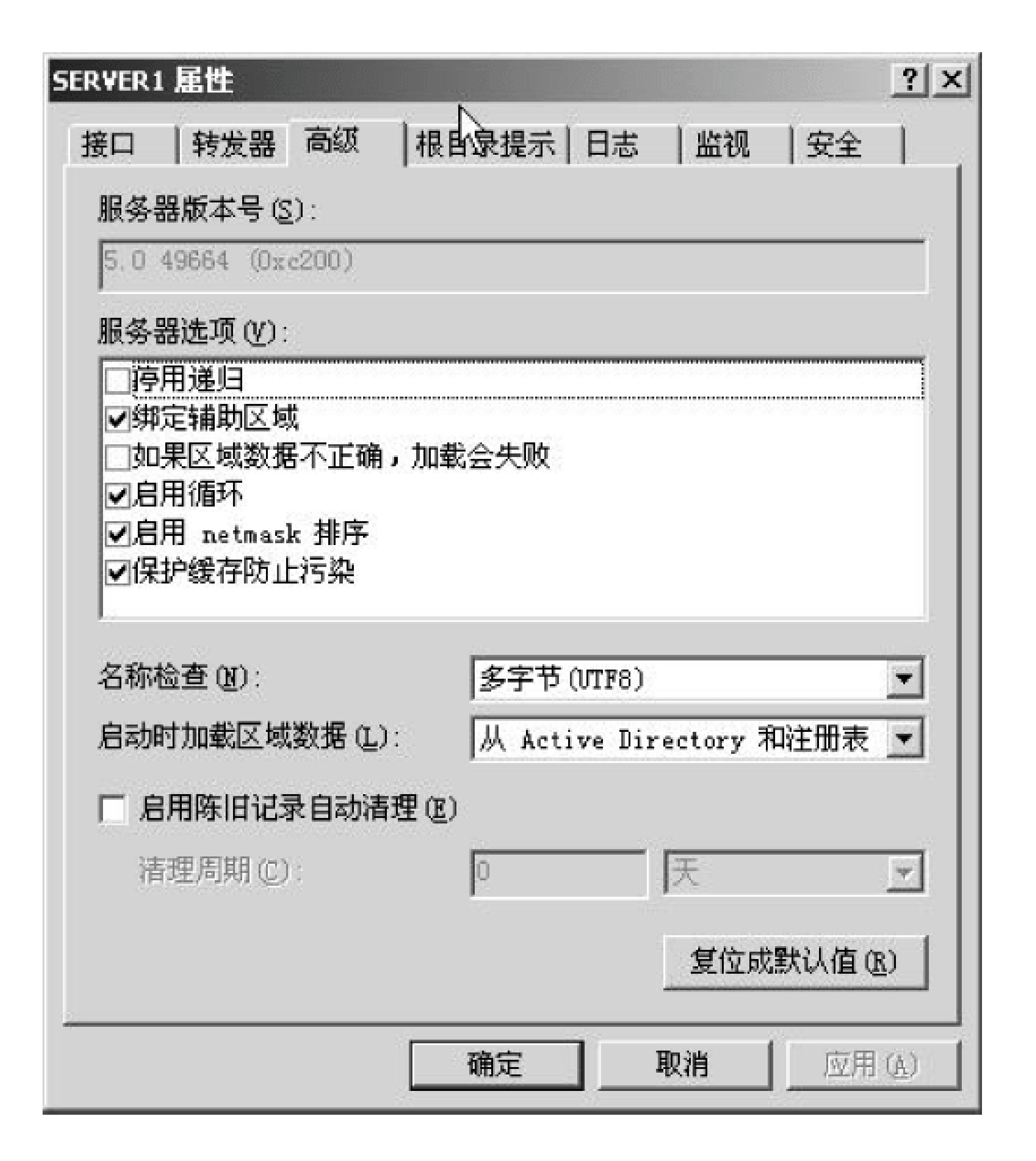


图 7-3　选取“保护缓存防止污染”选项

7.1.6　脚本和 ActiveX 攻击

脚本(Script)和 ActiveX 是近年来随着 Internet 的广泛使用而出现的攻击方法，也是目前危害最大的攻击之一。

1. 脚本攻击

脚本是一种可执行的文件，常见的编写脚本的语言有 Java Script 和 VB Script。脚本在执行时需要由一个专门的解释器来翻译成计算机指令，然后在本地计算机上运行。与 Java 和 VB 等编程语言相比，脚本编写简单，但功能较为强大。

脚本的另一个重要特点是可以直接嵌入到 Web 页面中。当执行一些静态 Web 页面时，脚本与之共同执行，可实现诸如数据库查询和修改及系统信息的提取等操作。脚本在带来方便和强大功能的同时，也为攻击者提供了方便的途径。攻击者可以编写一些对系统有破坏性的脚本，然后嵌入到 HTML 的 Web 页面中，一旦这些页面被下载到本地计算机，计算机便会以当前用户的权限执行这些脚本。当前用户所具有的任何权限，脚本都可以使用，由此可以看出脚本攻击的破坏程度很强。

2. ActiveX 攻击

ActiveX 是建立在微软公司的 COM(组件对象模型)上的一种控件对象，而 COM 则几乎是 Windows 操作系统的基础结构，它可以被应用程序加载，以完成一些特定的功能。但需要注意的是，这种对象控件不能自己执行，因为它没有自己的进程空间，而只能由其他进程加载。这时，这些控件便在加载进程的进程空间运行，类似于操作系统的可加载模块，例如 dll 库。

ActiveX 控件可以嵌入在 Web 页面中，当浏览器下载这些页面到本机后，相应地也下载了嵌入在其中的 ActiveX 控件，这样这些控件便可以在本地浏览器进程空间中运行。因此，当前用户的权限有多大，ActiveX 的破坏性便有多大。如果一个攻击者编写一个含有恶

意代码的 ActiveX 控件，然后嵌入在 Web 页面中，当被一个浏览用户下载并执行后，将会对本机造成破坏。

由于 ActiveX 对系统的操作没有严格的限制，所以如果一旦被下载并执行，就可以像安装在本机上的可执行程序一样干他们想干的事情。针对这一特点，IE 浏览器也作了某些限制，如图 7-4 和图 7-5 所示，针对那些不安全的站点，在 IE 浏览器的默认设置中将不允许用户进行下载或在下载时给予警告。目前，从事基于 ActiveX 开发的公司(如 VeriSign 公司)，他们对 ActiveX 控件进行了编号。当用户在下载控件时，IE 浏览器会给用户提示，并显示可信赖程度，由用户决定是否相信这个控件，以加强系统的安全性。



图 7-4　设置 IE 浏览器的安全属性

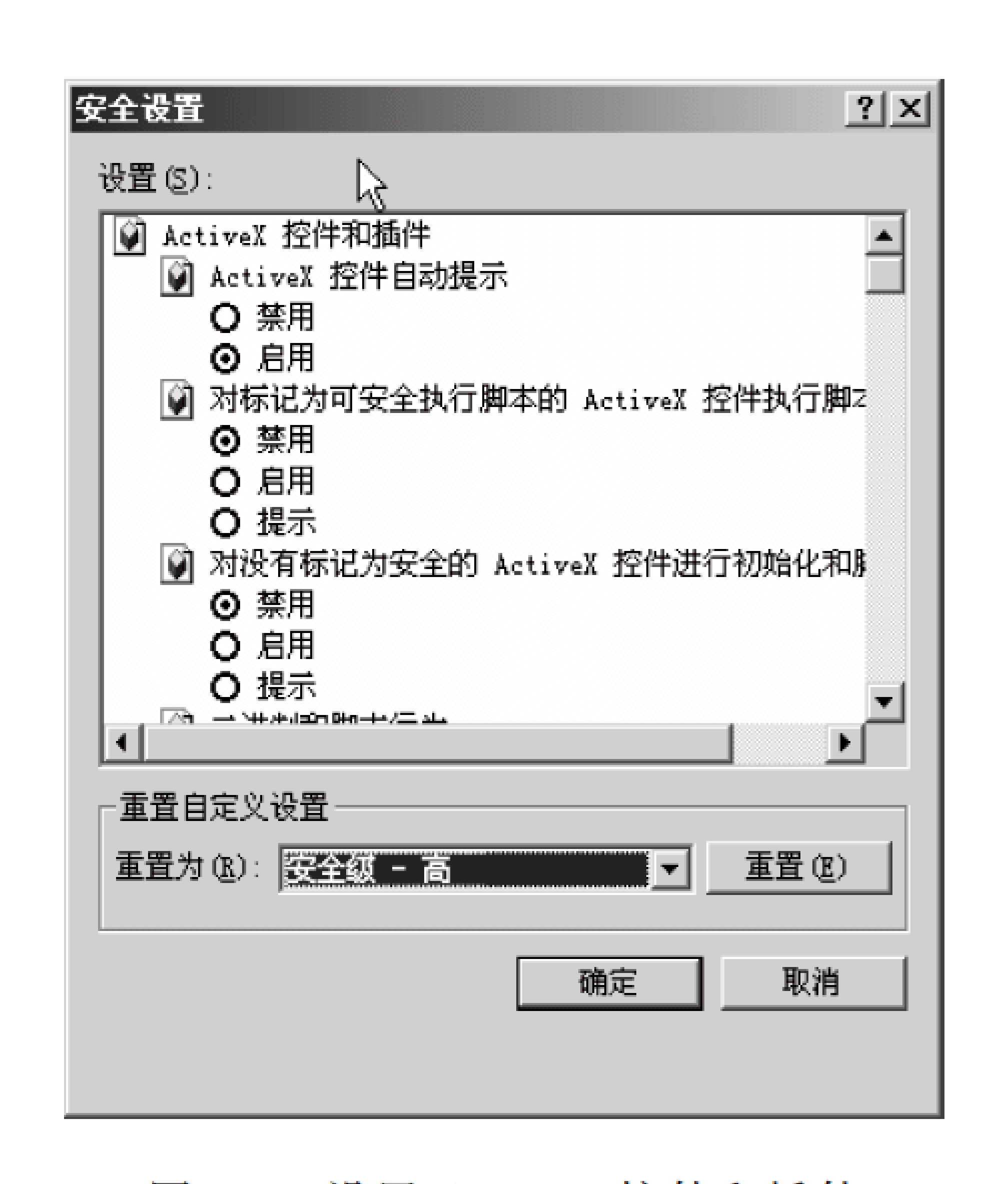


图 7-5　设置 ActiveX 控件和插件

在实际应用中，还有一些缺乏操作经验的用户，他们有时会不自觉地对 ActiveX 安全设置进行修改，让 ActiveX 控件在没有任何提示的情况下被下载安装，为网络安全带来隐患。

7.2　DoS 和 DDoS 攻击与防范

DoS(Denial of Servics，拒绝服务)和 DDoS(Distributed Denial of Servics，分布式拒绝服务)是两种常见的攻击方式，虽然实现原理比较简单，但产生的破坏性却较强。

7.2.1　DoS 攻击的概念

DoS 攻击是一种实现简单但又很有效的攻击方式。DoS 攻击的目的就是让被攻击主机拒绝用户的正常服务访问，破坏系统的正常运行，最终使用户的部分 Internet 连接和网络系统失效。最基本的 DoS 攻击就是利用合理的服务请求来占用过多的服务资源，从而使合法用户无法得到服务。DoS 攻击的原理如图 7-6 所示。

从图 7-6 可以看出，在 DoS 攻击过程中，首先攻击者向被攻击者发送大量带有虚假源地址的服务请求，被攻击者在接收到请求后返回确认信息，等待攻击者的确认，此过程需要

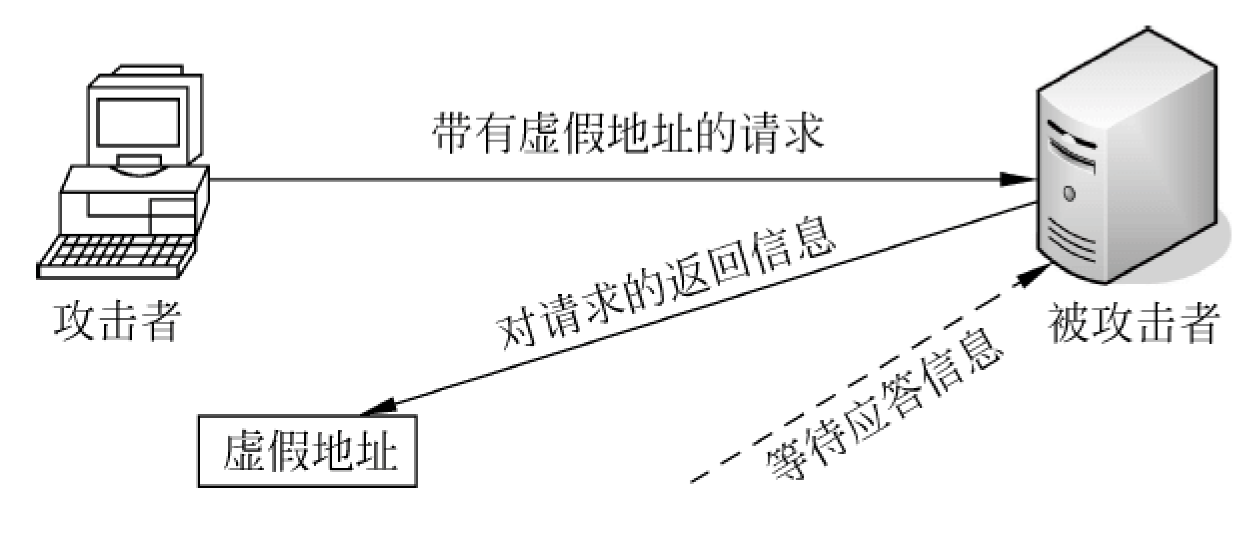


图 7-6　DoS 攻击的原理

TCP 的三次握手。由于攻击者所发送的请求的源地址是虚假的，所以被攻击者无法接收到确认(第三次握手)，一直处于等待状态，而分配给这次请求的资源却始终没有被释放。当被攻击者等待一定的时间后，连接会因超时而被断开，这时攻击者还会再度传送新的一批请求。在此过程中，被攻击者的资源最终会被耗尽，直到瘫痪。

7.2.2　DDoS 攻击的概念

DDoS 攻击是一种基于 DoS 攻击，但实现过程比较特殊的拒绝服务攻击方式。DDoS 是一种分布、协作的大规模攻击方式，主要用于对一些大型的网站或系统进行攻击。因为 DoS 攻击只是单机对单机的攻击，实现方法比较简单。与之不同的是，DDoS 攻击是利用一批受控制的主机向一台主机发起攻击，其攻击的强度和造成的威胁要比 DoS 攻击严重得多，当然其破坏性也要强得多。DDoS 攻击的原理如图 7-7 所示。

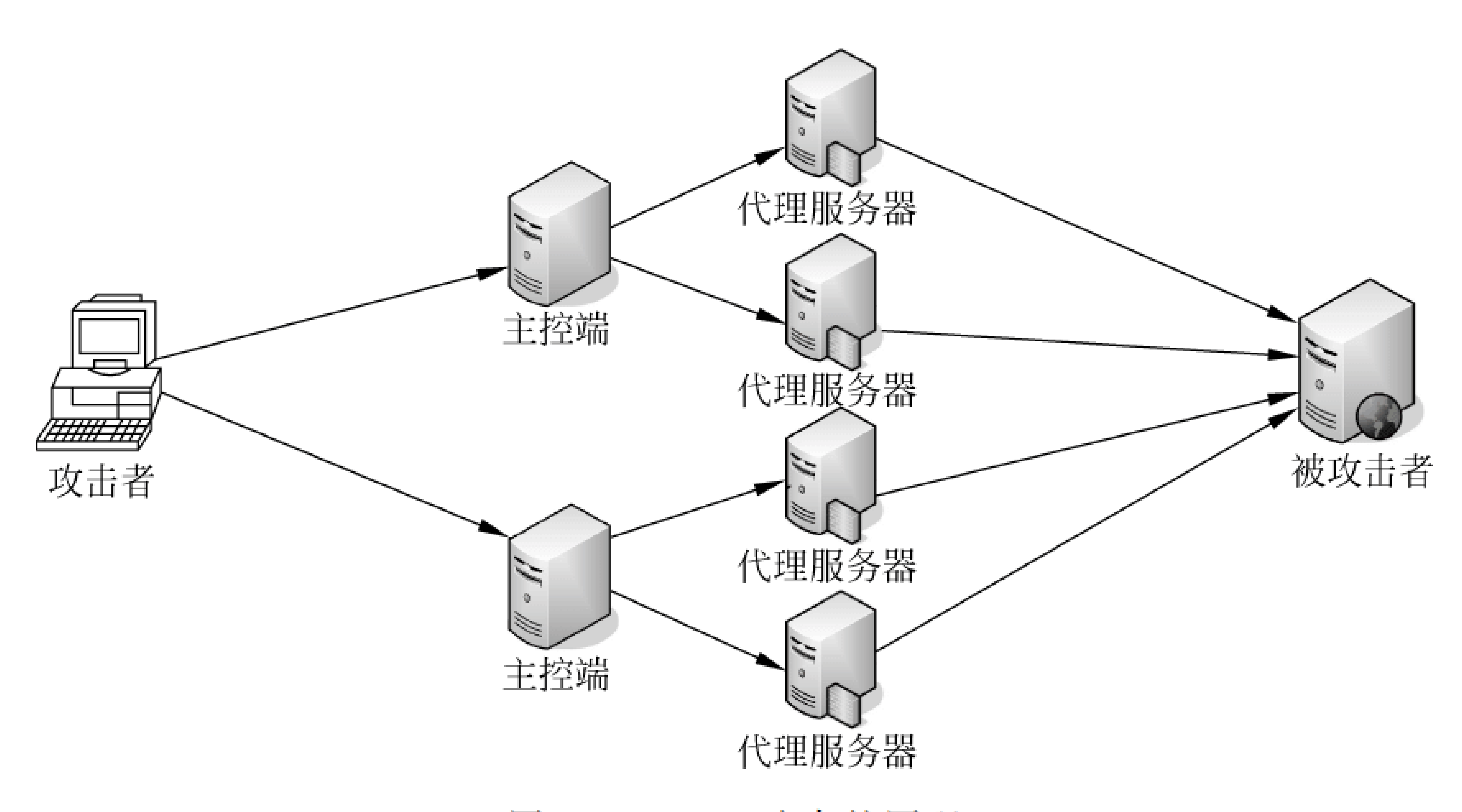


图 7-7　DDoS 攻击的原理

从图 7-7 可以看出，在整个 DDoS 攻击过程中，共由 4 部分组成：攻击者、主控端、代理服务器和被攻击者，其中每一个组成在攻击中扮演不同的角色。

(1) 攻击者。是指在整个 DDoS 攻击中的主控台，它负责向主控端发送攻击命令。与 DoS 攻击略有不同，DDoS 攻击中的攻击者对计算机的配置和网络带宽的要求并不高，只要能够向主控端正常发送攻击命令即可。

(2) 主控端。是攻击者非法侵入并控制的一些主机，通过这些主机再分别控制大量的代理服务器。攻击者首先需要入侵主控端，在获得对主控端的写入权限后，在主控端主机上安装特定的程序，该程序能够接受攻击者发来的特殊指令，并且可以把这些命令发送到代理服务器上。

（3）代理服务器。同样也是攻击者侵入并控制的一批主机，同时攻击者也需要在入侵这些主机并获得对这些主机的写入权限后，在上面安装并运行攻击程序，接受和运行主控端发来的命令。代理服务器是攻击的直接执行者，真正向被攻击主机发送攻击。

（4）被攻击者。是 DDoS 攻击的直接受害者，目前多为一些大型企业的网站或数据库系统。

在整个 DDoS 攻击过程中，攻击者发起 DDoS 攻击的第一步就是要寻找在 Internet 上有漏洞的主机，进入系统后安装后门程序，攻击者入侵的主机越多，参与攻击的主机也就越多。第二步是在入侵主机上安装攻击程序，其中一部分主机充当攻击的主控端，一部分主机充当攻击的代理服务器。最后各部分主机各司其职，在攻击者的统一指挥下对被攻击主机发起攻击。由于攻击者在幕后操纵，所以在攻击时不会受到监控系统的跟踪，身份不容易被发现。

7.2.3 利用软件运行缺陷的攻击和防范

在实际应用中没有一款软件在安全特性上是十全十美的，任何一款软件都存在这样或那样的缺陷，其中有些缺陷在其运行过程中被反映出来。如果这些缺陷被攻击者发现，就会用来进行攻击。由于软件在开发过程中对某种特定类型的报文或请求没有进行较好的处理，导致这些软件在遇到这种类型的报文时将会出现异常，导致软件本身或系统崩溃。这类攻击有其特殊性，故在这里进行单独介绍。

利用软件运行缺陷进行 DoS 攻击的工具主要有 teardrop 攻击（如 teardrop.c、boink.c 和 bonk.c 等）、LAND 攻击和 ICMP 碎片包攻击等，另外还有针对 Cisco 路由器 IOS version 12.0(10)远程拒绝服务攻击的专用工具等。这些攻击都是利用了被攻击软件在实现过程中存在的缺陷而进行的。例如，teardrop.c 攻击工具可通过以下的命令对其他主机进行 DoS 攻击。

```
teardrop ＜源 IP＞ ＜目标 IP＞ [-s 源端口] [-d 目的端口] [-n 次数]
```

从 Windows NT 开始，当系统未及时安装补丁程序时，就可以使用一些专用工具进行 DoS 攻击。例如，SMBdie.exe 就是针对 Windows 的 SMB 实现的 DoS 攻击，可以对 Windows NT/2000/XP/2003 NetBIOS(139)进行攻击，该工具在局域网中使用非常有效，操作界面如图 7-8 所示。

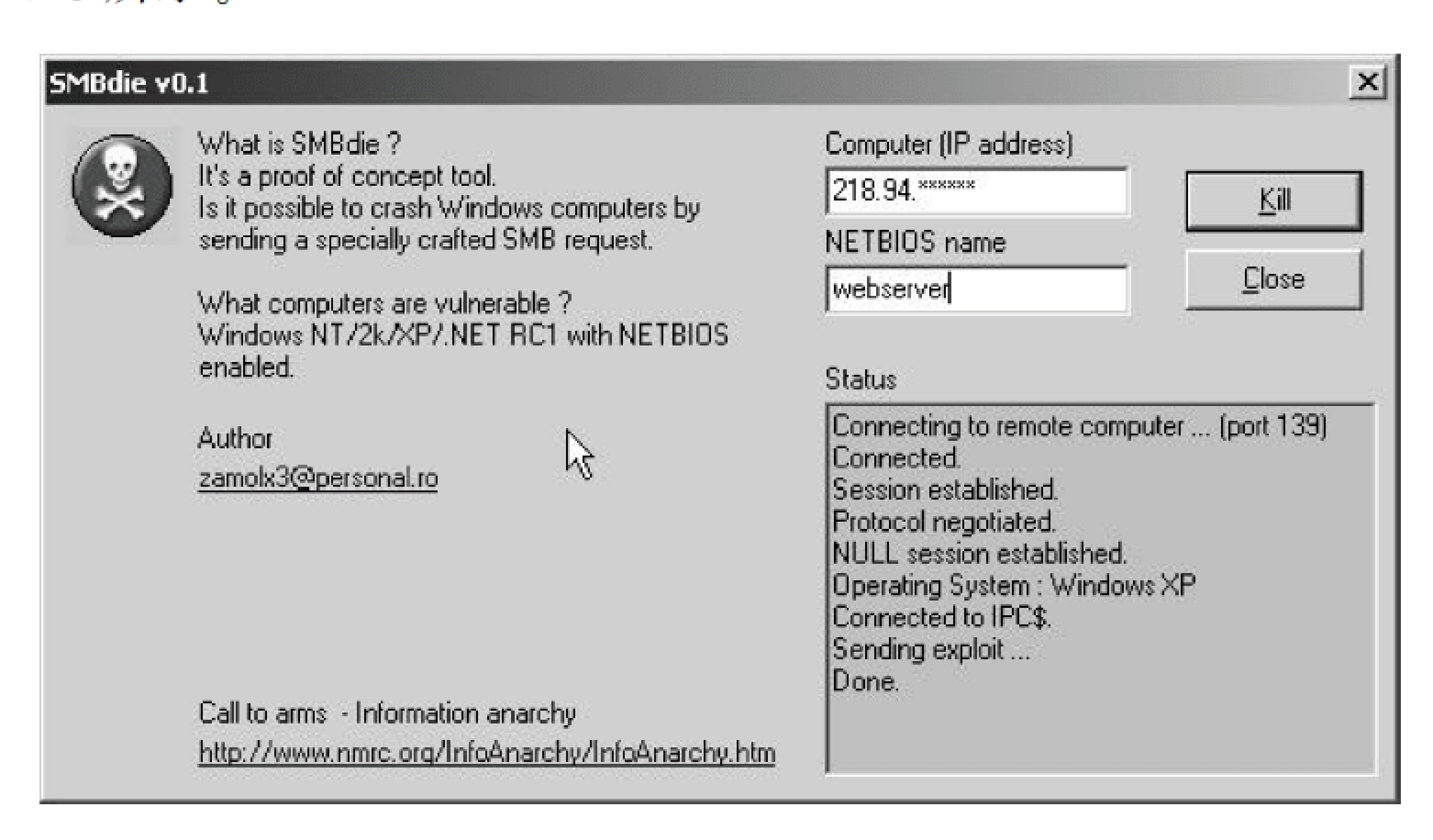


图 7-8 SMBdie 攻击界面

SMB(Server Message Block,服务器信息块)用于在 Windows 操作系统中实现资源共享,包括共享文件、文件夹、磁盘和打印机等,在某些情况下甚至可以共享 COM 端口。一个 SMB 客户机或服务器可以和多种机器和网络相互连接。

从上面的介绍可以看出,这种攻击行为威力很大,而且难于察觉。不过,由于这种攻击主要是针对软件运行中的缺陷而实现的,所以对于用户来说最有效的防范这类 DoS 攻击的方法是及时安装软件的补丁程序。例如,对于大家普遍使用的 MS SQL、Oracle 等数据库,建议能够及时安装相应的补丁程序,以防止 DoS 攻击,增强其运行的安全性。

7.2.4 利用防火墙防范 DoS/DDoS 攻击

DoS 攻击是一种很简单但又很有效的网络攻击方式,它可以利用合理的服务请求来占用对方过多的服务资源,从而使合法用户无法得到服务。DDoS 攻击是一种基于 DoS 的特殊形式的拒绝服务攻击方式,攻击者通过事先控制大批主控端和代理服务器(将主控端和代理服务器通常称为"傀儡机"),并控制这些主机同时发起对目标主机的 DoS 攻击,具有较大的破坏性。

从实际应用来看,防火墙是抵御 DoS/DDoS 攻击最有效的设备。因为防火墙的主要功能之一就是在网络的关键位置对数据包进行相应的检测,并判断数据包是否被放行。下面说明防火墙在各种网络环境中对 DoS/DDoS 攻击的有效防范方法。

1. 通过基于状态的资源控制来保护内网资源

目前绝大多数主流防火墙(如 Cisco PIX、NetScreen 和 SmartHammer 等)都支持 IP Inspect(IP 检测)功能,防火墙会对进入防火墙的信息进行严格的检测。这样,各种针对系统漏洞的攻击包(如前面介绍的 Ping of Death、TearDrop 等)会自动被系统过滤掉,从而保护了网络免受来自于外部的漏洞攻击。对防火墙产品来说,资源是十分宝贵的,当受到外来的 DDoS 攻击时,系统内部的资源全都被攻击数据包所占用,此时正常的服务请求和响应肯定会受到影响。防火墙基于状态的资源控制会自动监视网络内所有的连接状态,当发现存在连接长时间但还未得到应答的处于半连接状态(即未完成第三次握手)的数据包超过预设置的范围时,就判断有可能遭受到了 DoS/DDoS 攻击,从而清除所有的半连接状态。另外,在此过程中还可以通过以下的策略来优化系统配置。

(1) 有些防火墙可以控制连接与半连接的超时时间,必要时还可以缩短半连接的超时时间,以加速半连接的老化。

(2) 限制系统各个协议的最大连接数,保证协议的连接总数不超过系统限制值,在达到连接值的上限后自动删除新建的连接。

(3) 针对源或目标 IP 地址做流量限制。检测功能可以限制每个 IP 地址的资源,用户在资源控制范围内的使用并不会受到任何影响。但当用户感染了蠕虫病毒或发送攻击报文时,针对流的资源控制可以限制每个 IP 地址发送的连接数目,超过限制的连接将被丢弃。这种做法可以有效地抑制病毒产生攻击的效果,避免其他正常使用的用户受到影响。

(4) 单位时间内如果穿过防火墙的"同类"数据流超过已设置的上限值后,可以设定对该类数据流进行阻断。这样可以有效防御对于 IP、ICMP 和 UDP 等非连接的泛洪攻击。

2. 防范 SYN 泛洪

SYN 泛洪(SYN Flood)是 DDoS 攻击中危害性最强也是最难防范的一种攻击方法。

SYN 泛洪攻击利用 TCP 协议缺陷，发送大量伪造的 TCP 连接请求，从而使得被攻击方资源耗尽(CPU 满负荷或内存不足)。不同品牌的防火墙处理 SYN flood 攻击的方法可能存在实现细节上的不同。例如，SmartHammer 系列防火墙便利用智能 TCP 代理技术来判断连接的合法性，从而保护网络资源，其工作原理如图 7-9 所示。

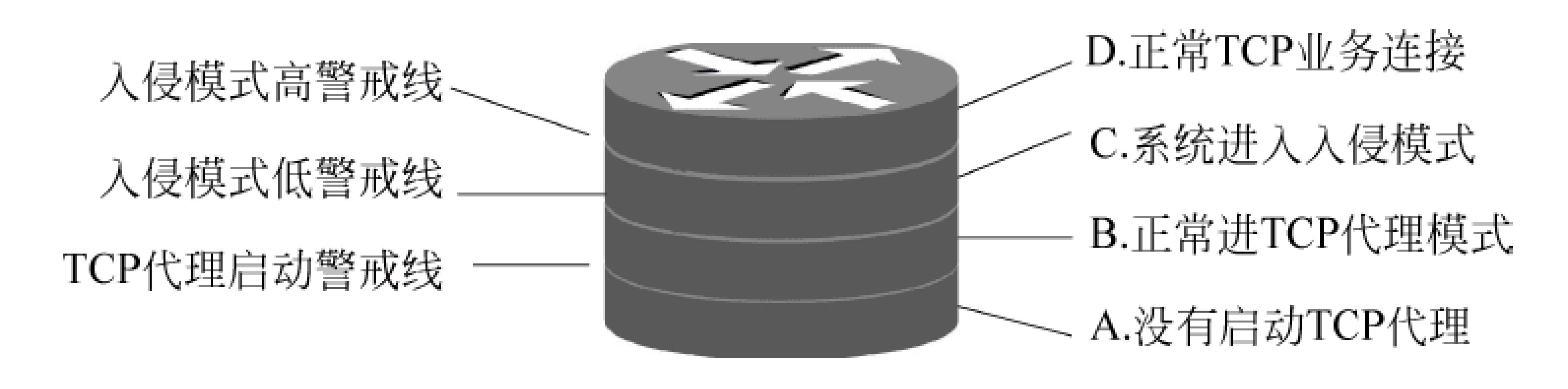


图 7-9　TCP 代理技术的工作原理

从图 7-9 可以看出，防火墙正常工作时并不会立即开启 TCP 代理(以免影响速度)，只有当网络中的 TCP 半连接数量达到系统设置上限(TCP 代理启动警戒线)时，正常的 TCP Intercept 才会自动启动，并且当系统的 TCP 半连接超过系统 TCP Intercept 高警戒线时，系统进入入侵模式，此时新建立的连接会覆盖原有的 TCP 连接。此后，系统全连接数增多，半连接数减小，当半连接数降到入侵模式低警戒线时，系统退出入侵模式。如果此时攻击停止，系统半连接数量逐渐降到 TCP 代理启动警戒线以下，智能 TCP 代理模块停止工作。通过智能 TCP 代理可以有效防止 SYN 泛洪攻击，保证网络资源安全。

3. 利用 NetFlow 对 DoS 攻击和病毒监测

在介绍 NetFlow 之前，先来介绍一下 Flow。Flow 是网络设备厂商为了在设备内部提高路由转发速度而引入的一项技术，其本意是将高 CPU 消耗的路由表软件查询匹配作业部分转移到硬件实现的快速转发模块上(如 Cisco 的 CEF 模式)。在这种功能模式中，数据包将通过几个给定的特征定义合并到特定的集合中，这个集合就是 Flow。目前，Flow 数据被广泛用于高端网络流量测量技术中，以提供网络监控、流量图式分析、应用业务定位、网络规划、快速排错、安全分析(如 DDoS 攻击)和域间记账等数据挖掘功能。在实际软件实现中，Flow 所包含的字段定义及数量将会随着厂商甚至协议版本的不同而出现变化，业界因此也相应出现了各种不同的实现版本。而在这些不同的 Flow 版本中，NetFlow 得益于 Cisco 公司在网络设备行业内的领先地位而获得最大范围的认同，为此目前多使用 NetFlow。

网络监控在抵御 DoS/DDoS 攻击中有着重要的意义。目前主流的防火墙一般都支持 NetFlow 功能，它将网络交换中的数据包识别为流的方式加以记录，并封装为 UDP 数据包发送到分析器上，这样就为网络管理、流量分析和监控、入侵检测等提供了丰富的信息来源。可以在不影响转发性能的同时记录、发送 NetFlow 信息，并能够利用网络安全管理平台对接收到的资料进行分析、处理。利用 NetFlow 可以完成以下的操作。

(1) 监视网络流量。防火墙可以有效地抵御 DoS/DDoS 攻击，当攻击流数量已经完全占据了带宽时，虽然防火墙已经通过安全策略把攻击数据包丢弃，但由于攻击数据包已经占据了所有的网络带宽，正常的用户访问依然无法完成。此时网络的流量是很大的，防火墙可以利用内置的 NetFlow 统计分析功能，查找攻击流的数据源，并告知网络管理员，对数据流分流或导入黑洞路由。通过在防火墙相关接口(一般为外网连接接口，也可以是内网连接接口)中开启 NetFlow 采集功能，并设置 NetFlow 输出服务器地址，这样就可以利用安全管理

平台对接收的信息进行分析处理,并以此为标准,当发现网络流量异常的时候,就可以利用NetFlow有效地查找、定位DDoS攻击的来源。

(2)监视蠕虫。防止蠕虫的攻击,重要的是防止蠕虫病毒的入侵,只有尽早发现,才可以迅速采取措施有效阻止。各种蠕虫在感染了系统后,为了传播自身,会主动向外发送特定的数据包并扫描相关端口。目前主流的防火墙多集成了蠕虫查询模板,定期查询,当发现了匹配的蠕虫时,可以分析该地址是否已经感染了病毒,然后采取相应的措施。

7.3 IDS技术及应用

随着网络安全技术的发展,入侵检测系统(Intrusion Detection System,IDS)在网络环境中的应用越来越普遍。本节将介绍入侵检测技术的相关概念、信息的采集、规则的建立和实现等内容。

7.3.1 IDS的概念及功能

国家标准GB/T 18336《信息技术安全性评估准则》对入侵检测(intrusion detection)的定义为"通过对行为、安全日志或审计数据或其他网络上可以获得的信息进行操作,检测到对系统的闯入或闯入的企图"。入侵检测技术是为保证计算机系统的安全而设计与配置的一种能够及时发现并报告系统中未授权或异常现象的技术,是一种用于检测计算机网络中违反安全策略行为的技术。进行入侵检测的软件与硬件的组合便是入侵检测系统。

1. 入侵检测的功能

入侵检测的功能如下。

(1)监督并分析用户和系统的活动。

(2)检查系统配置和漏洞。

(3)检查关键系统和数据文件的完整性。

(4)识别代表已知攻击的活动模式。

(5)对反常行为模式的统计分析。

(6)对操作系统的校验管理,判断是否有破坏安全的用户活动。

2. 入侵检测系统的特点

入侵检测系统的使用特点如下。

(1)提高信息安全体系整体的完整性。

(2)提高系统的监察能力。

(3)跟踪用户从进入到退出的所有活动或影响。

(4)识别并报告数据文件的改动。

(5)发现系统配置的错误,必要时予以更正。

(6)识别特定类型的攻击,并向相应人员报警,以作出防御反应。

(7)可使系统管理人员能够将最新的版本升级添加到程序中。

(8)为信息安全策略的创建提供指导。

3. 入侵检测系统存在的不足

入侵检测系统存在的不足如下。

(1)在无人干预的情况下,无法执行对攻击的检查。

（2）无法感知公司安全策略的内容。

（3）不能弥补网络协议的漏洞。

（4）不能弥补系统提供的原始信息的质量缺陷或完整性问题。

（5）不能分析网络繁忙时所有的事务。

（6）不能总是对数据包级的攻击进行处理。

（7）不能应付现代网络的硬件及特性。

入侵检测作为一种积极主动的安全防护技术，提供了对内部攻击、外部攻击和误操作的实时保护，在网络系统受到危害之时拦截和响应入侵。

7.3.2 IDS中的相关术语

随着IDS技术的发展，与之相关的术语相应出现，且同一术语也在发生着不同程度的变化，下面介绍与IDS技术相关的一些基本术语。

1. Alerts（报警）

当一个入侵正在发生或者试图发生时，IDS系统将发布一个报警信息通知系统管理员。对于IDS来说，Alert信息一般是通过远程控制台来显示。其中，IDS与远程控制台之间可以通过SNMP（简单网络管理协议）、E-mail、SMS（短信息）中的一种或几种方式中的多种方式的组合来传递给管理员。在报警中，可分为错误的报警和正确的报警两种。其中，错误报警又分为误报和漏报两种。

（1）误报。当IDS工作于正常的状态下所生产的报警称为误报。误报使网络管理员浪费宝贵的时间和资源来分析根本不存在的攻击。所以，网络管理员需要正确设置IDS的报警参数。如果一个IDS经常发生误报，这样时间一长就可能会降低管理员的敏感性，当有正确的报警产生时可能会被管理员疏忽，或处理不及时。此现象类似于民间传说的“狼来了”的故事。

（2）漏报。IDS对已知的入侵活动未产生报警的现象称为漏报。漏报说明IDS虽然在进行攻击的检测，但它却没有命中真正的攻击。大多数IDS都通过相关技术尽量使系统避免漏报，但完全清除漏报是很困难的，基本是不可能的。由于漏报会导致攻击者能够实现攻击过程，但IDS却没有检测到，这对网络系统会产生严重的安全威胁。一般情况下，漏报是因为IDS的软件缺陷所导致的。

2. Attacks（攻击）

Attacks指试图渗透系统或绕过系统的安全策略以获取信息、修改信息，以及破坏目标网络或系统功能的行为。下面列出的是IDS能够检测出的最常见的Internet攻击类型。

（1）DoS攻击（Denial of Service attack，拒绝服务攻击）。DoS攻击是通过一种直接的破坏方式使系统瘫痪，或使系统无法给用户提供正常的服务。

（2）DDoS攻击（Distributed Denial of Service attack，分布式拒绝服务攻击）。因为DoS攻击一般是通过一台主机来攻击另一台远程主机，所以DoS攻击产生的效果相对较弱。而DDoS攻击利用了分布式系统的特点，攻击者通过多台分散的主机向一台目标主机发动攻击，耗尽远程主机的资源，或者使其连接失效。

（3）Smurf。这是一种出现较早的攻击方式，攻击者使用被攻击主机的IP地址来伪装源地址，并向一个smurf放大器（Smurf Amplifier）的广播地址执行ping操作，然后所有活

动主机都会向该被攻击主机发送应答信息,从而使被攻击主机中断网络连接。

(4) Trojans(特洛伊木马)。在计算机术语中,木马原本是指那些以合法程序的形式出现,其实包藏了恶意软件的那些软件。这样,当用户运行合法程序时,在不知情的情况下,恶意软件就被安装并运行。

7.3.3 IDS 的分类

根据不同的标准,可以对 IDS 进行不同的分类。下面主要从 IDS 的工作原理对其进行类别划分。根据实现技术的不同,IDS 可以分为异常检测模型、误用检测模型和混合检测模型三种类型。

1. 异常检测模型

异常检测(anomaly detection)模型主要检测与可接受行为之间的偏差。如果可以预先定义每项可接受的行为(如对 HTTP 的正常访问、正常的 TCP 连接及正常的 SMTP 协议使用等),那么每项不可接受的行为(如 TCP 半连接状态、大量连续的 SMTP 连接等)就应该是入侵。首先总结正常操作应该具有的特征(用户轮廓),当用户活动与正常行为有重大偏离时即被认为是入侵。这种检测模型的漏报率低,但误报率高。因为不需要对每种入侵行为进行定义,所以能有效检测未知的入侵。

2. 误用检测模型

误用检测(misuse detection)模型主要检测与已知不可接受行为之间的匹配程度。如果可以定义所有的不可接受行为,那么每种能够与之匹配的行为都会引起报警。收集非正常操作的行为特征,建立相关的特征库,当监测的用户或系统行为与库中的记录相匹配时,系统就认为这种行为是入侵。误用检测型检测基于已知的系统缺陷和入侵模式,所以又称“特征检测模型”。它能够准确地检测到某些特征的攻击,但却过度依赖事先定义好的安全策略,所以无法检测系统未知的攻击行为,从而产生入侵或攻击的漏报。

3. 混合检测模型

混合检测模型是对异常检测模型和误用检测模型的综合。近几年来,混合检测模型日益受到人们的重视。这类检测在做出决策之前,既分析系统的正常行为,同时还观察可疑的入侵行为,所以判断结果更全面、准确和可靠。

混合检测并不为不同的入侵行为分别建立模型,而是首先通过大量的事例学习什么是入侵行为及什么是系统的正常行为,发现描述系统特征的一般使用模式,然后再形成对异常和误用都适用的检测模型。

7.3.4 IDS 的信息收集

入侵检测的第一步是信息收集,收集内容包括系统、网络、数据及用户活动的状态和行为。此工作由放置在不同网段的传感器或不同主机上的代理来进行,包括系统和网络日志文件、网络流量及非正常的目录和文件改变及非正常的程序执行等。

1. 信息收集的方法

就准确性、可靠性和效率而言,IDS 收集到的信息是它进行检测和决策的基础。如果收集信息的时延太大,很可能在检测到攻击的时候,入侵者已经完成了入侵过程;如果信息不完整,系统的检测能力就会下降;如果信息本身不正确,系统就无法检测到某些攻击,从而

给用户形成一种不真实的安全感。所以研究信息收集机制是非常重要的。根据对象的不同,信息收集的方法包括基于主机的信息收集、基于网络的信息收集和混合型信息收集三种类型。

1）基于主机的信息收集

系统分析的数据是计算机操作系统的事件日志、应用程序的事件日志、系统调用、端口调用和安全审计记录。主机型入侵检测系统保护的一般是所在的主机系统。是由代理(agent)来实现的,代理是运行在目标主机上的可执行程序,它们与命令控制台(console)通信。基于主机的 IDS 部署如图 7-10 所示。

2）基于网络的信息收集

系统分析的数据是网络上的数据包。网络型入侵检测系统担负着保护整个网段的任务,基于网络的入侵检测系统由遍及网络中每个网段的传感器(sensor)组成。传感器是一台将以太网卡置于混杂模式的计算机,用于嗅探网络上的数据包。基于网络的 IDS 部署如图 7-11 所示(当单位内部网络存在多个网段时,建议在每一个网段分别安装一个传感器)。

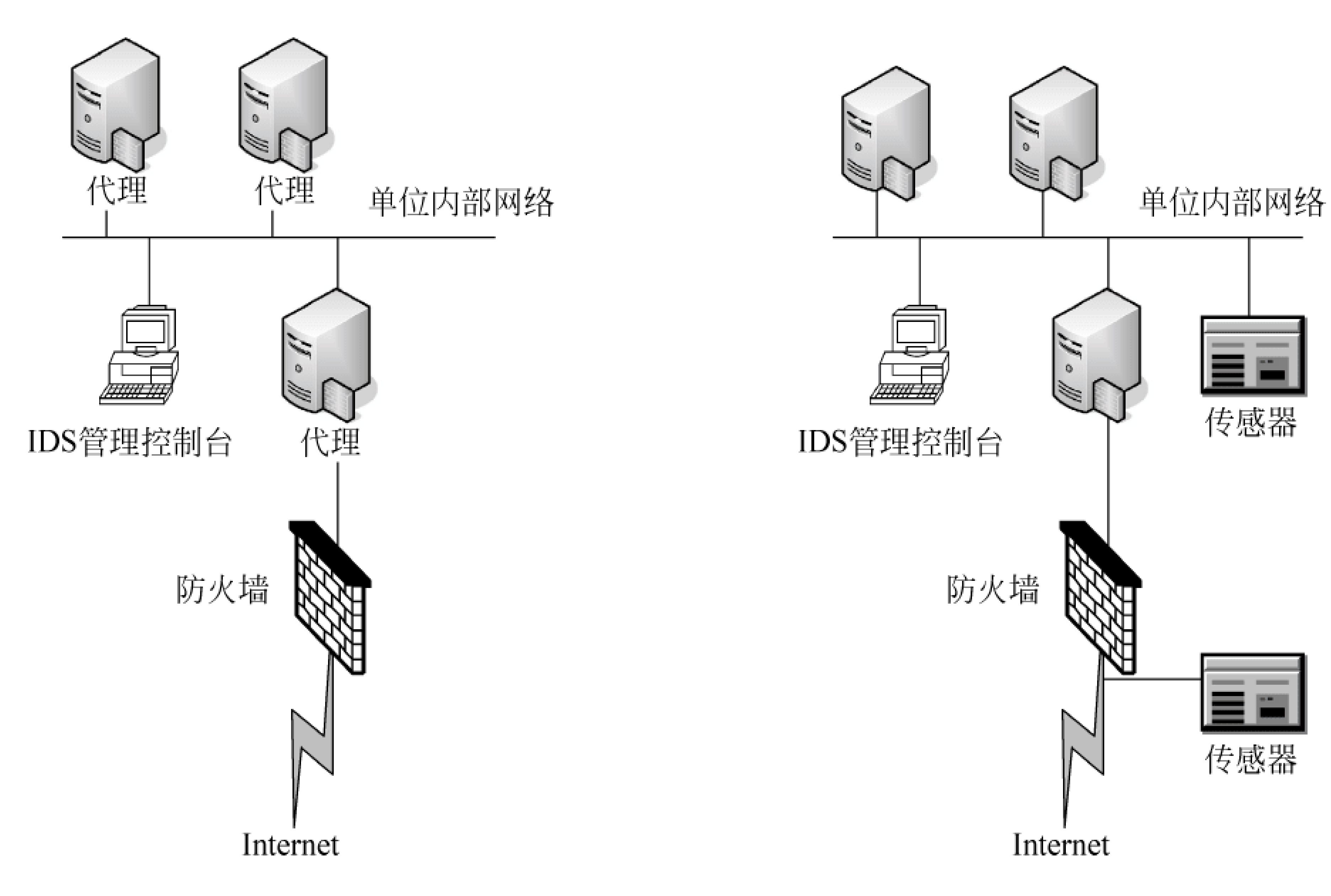


图 7-10　基于主机的 IDS 部署　　图 7-11　基于网络的 IDS 部署

3）混合型信息收集

混合型信息收集是基于网络的信息收集和基于主机的信息收集的有机结合。基于网络的信息收集和基于主机的信息收集都存在不足之处,会造成防御体系的不全面,而混合型入侵检测系统既可以发现网络中的攻击信息,也可以从系统日志中发现异常情况。

基于网络的数据收集有时会比基于主机的数据收集效果更好,尤其是主机对攻击行为没有反应的时候(例如,攻击数据包指向的端口是关闭的),也可以通过终端主机网络协议的底层检测到这些攻击。总体而言,基于主机的数据收集占有一定的优势。

① 基于主机的信息收集所收集到的数据能准确反映主机上发生的情况,而不是根据从网络上收集到的数据包去猜测发生了什么事情。

② 在数据流量很大的网络中,由于受线路的影响,网络监视器经常会产生丢包,但主机

监视器则可以报告每台主机上发生的所有事件。

③ 基于网络的信息收集机制对插入攻击和规避攻击无能为力，但基于主机的信息收集就不存在这样的问题，它能够处理主机收到的所有数据。

2. 直接监控与间接监控

信息收集的途径分为直接监控和间接监控。

(1) 直接监控。从信息生成地或属地直接获取数据。例如，如果要直接监控某台主机的 CPU 负载情况，就需要从主机相应的内核结构中获取数据。

(2) 间接监控。从能反映监控目标行为的数据源处获取数据。例如，如果要直接监控某台主机的 CPU 负载情况，间接监控可以通过读取记录 CPU 负载的日志文件，完成对主机 CPU 负载的监控。

就检测入侵行为而言，直接监控要优于间接监控，原因如下。

(1) 从非直接数据源获取的数据(如审计踪迹)在被 IDS 使用之前，有被入侵者修改的潜在可能。尤其是通过未加密的以明文方式传输和存储的数据被篡改的可能性更大。

(2) 非直接数据源可能无法记录某些事件。

(3) 在间接监控中，数据一般都是通过某种机制生成的(如编写审计踪迹的代码)，但那些机制并不了解 IDS 使用数据的具体需求。因此，从间接数据源获取的数据量总是非常大，一个 C2 级生成的审计踪迹可能包含每个用户每天 50～500KB 的记录，对于一个中等规模的用户组来说，每天审计踪迹数据可能会有好几百兆。由于这个原因，IDS 在使用间接数据源时，通常必须消耗大量的资源对数据进行过滤和精简。直接监控方法只获取它需要的数据，所以生成的数据量相对较小。此外，监控组件自身也会对数据进行分析，只有在检测到相关事件时才产生结果，这样就减少了数据的存储量。

(4) 间接监控机制的伸缩性差。因为当主机及其内部被监控要素的数目增加时，过滤数据的开销会降低被监控主机的性能。

(5) 间接数据源常常在数据产生和 IDS 访问这些数据之间有一个时延，而直接监控的时延就小得多，这样 IDS 才能据此做出更及时的响应。

3. 信息收集的渠道

IDS 目前所能检测到的大部分入侵都是由主机上的活动引起的，如执行某一命令、访问某项服务并提供不正确的数据等，这些攻击活动发生在终端机上，有时通过网络检测也可以发现。针对网络本身的攻击通常都是数据流，即发送的数据量超过网络的承受能力，以至于合法数据包通信受阻。但在终端机上也照样可以检测到这些攻击，例如通过查看主机 ICMP 报文是否有大量的 Echo-Request 分组，也可以检测到是否有 Ping 的泛洪数据流攻击发生。入侵检测利用的信息一般来自以下 4 个方面。

1) 系统和网络日志文件

攻击者经常在系统日志文件中留下他们的踪迹，因此充分利用系统和网络日志文件信息是检测入侵的必要条件。日志中包含发生在系统和网络上的不寻常和不期望活动的证据，这些证据可以指出有人正在入侵或已成功入侵了系统。通过查看日志文件，能够发现成功的入侵或入侵企图，并很快地启动相应的应急响应程序。日志文件中记录了各种行为类型，每种类型又包含不同的信息。例如记录“用户活动”类型的日志，就包含登录、用户 ID 改变、用户对文件的访问、授权和认证信息等内容。很显然，不正常的或不期望的用户行为就

是重复登录失败、登录到不期望的位置及非授权的企图访问重要文件等。图 7-12 所示的是通过 Windows Server 2003 的“事件查看器”记录的相关日志，网络管理员要养成经常查看日志记录的习惯。

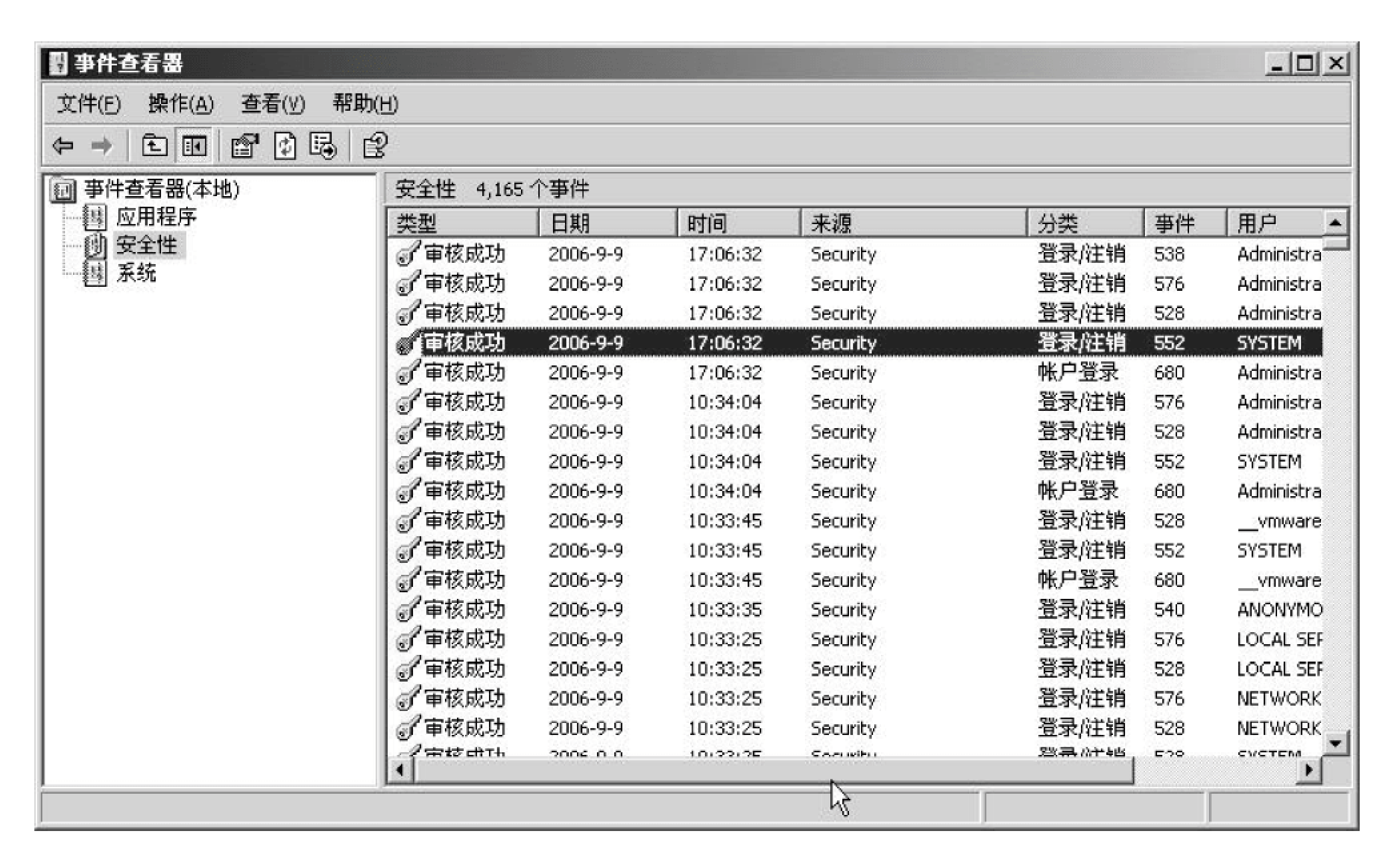


图 7-12　Windows Server 2003 的日志记录

2）目录和文件中不期望的改变

网络环境中的文件系统包含很多软件和数据文件，保存有重要信息的文件经常是入侵者获取、修改或破坏的目标。目录和文件中不期望的改变（包括修改、创建和删除），很可能就是一种入侵产生的指示和信号。对于 FTP 服务器来说，会根据不同的用户来对指定的目标分配相应的权限。如果给某些用户仅指定了“读取”权限（如图 7-13 所示），但却发现该用户对应的目录下产生了大量的文件或文件夹，这很可能就是有入侵者行为发生。

另外，出于安全考虑，当在网络中共享某些资源时，会在共享名后加 $ 符号以对共享资源进行隐藏，这样只有知道完整的共享名称的用户才能访问，如图 7-14 所示。但是，如果发现这些已设置了隐藏的文件夹中突然出现了一些不明的文件，或某些文件被修改，也可能是入侵者所为。

3）程序执行中的不期望行为

网络系统上的程序执行一般包括操作系统、网络服务和特定的应用程序。每个在系统上执行的程序对应一到多个进程。每个进程的执行都拥有不同的环境，特殊的环境决定了进程可访问的系统资源（如硬盘空间、外设等）、程序和数据文件等。一个进程的运行由它对应的操作来体现，操作执行的方式不同，利用的系统资源也就不同。操作包括计算、文件传输，以及与网络中其他进程的通信等。一个进程出现了不期望的行为可能表明攻击者正在入侵或用户的系统已被入侵。一般情况下，入侵者在进入用户的系统后，为了安全地运行后门程序，会将该程序运行时进程修改为系统中已有的进程。所以，对于熟悉的一些进程的运行状态也要引起网络管理员的关注，当某一进程出现异常（如 CPU 占用率突然持续保持在较高的水平）时，就要查看该进程提供的服务。

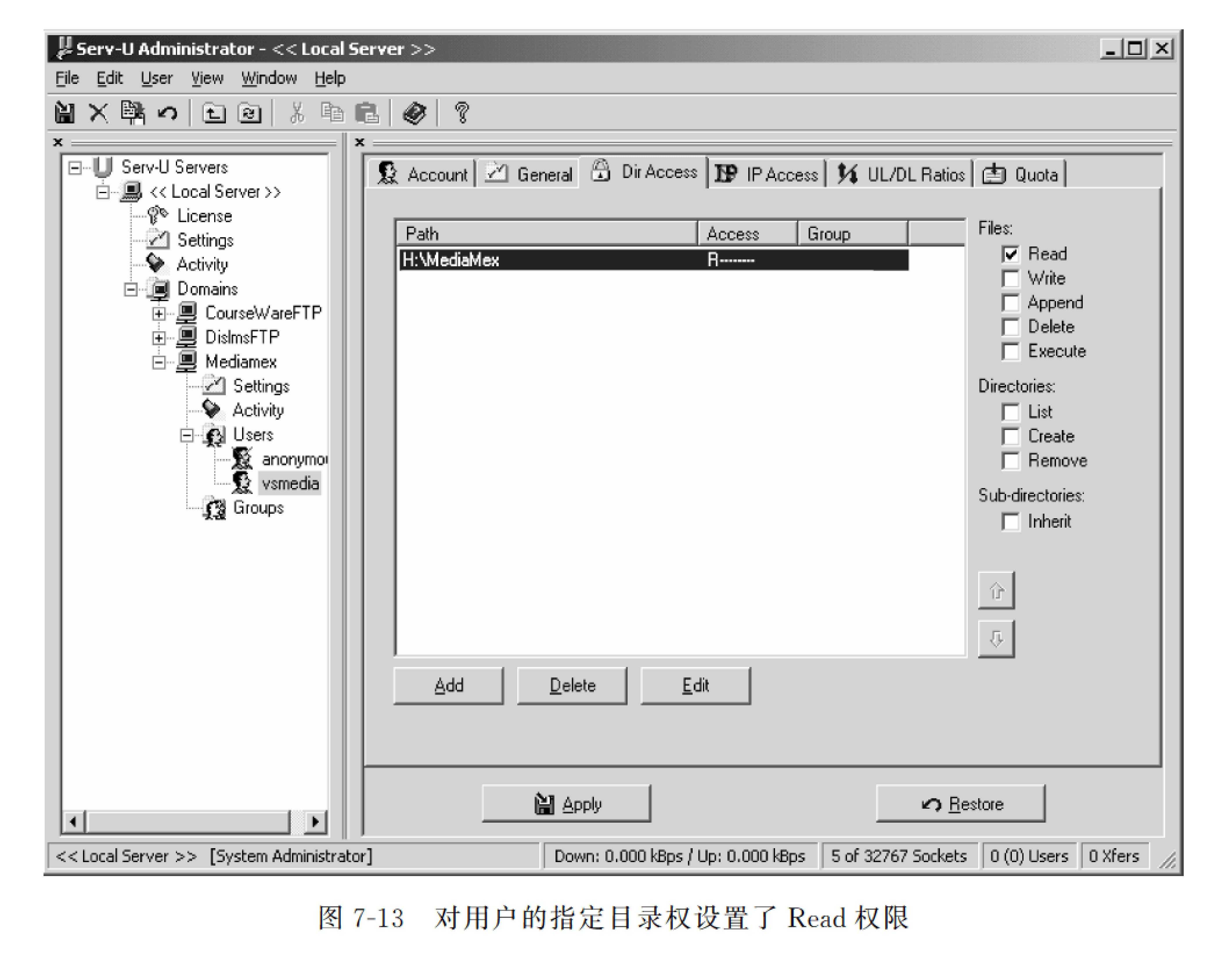


图 7-13　对用户的指定目录权设置了 Read 权限

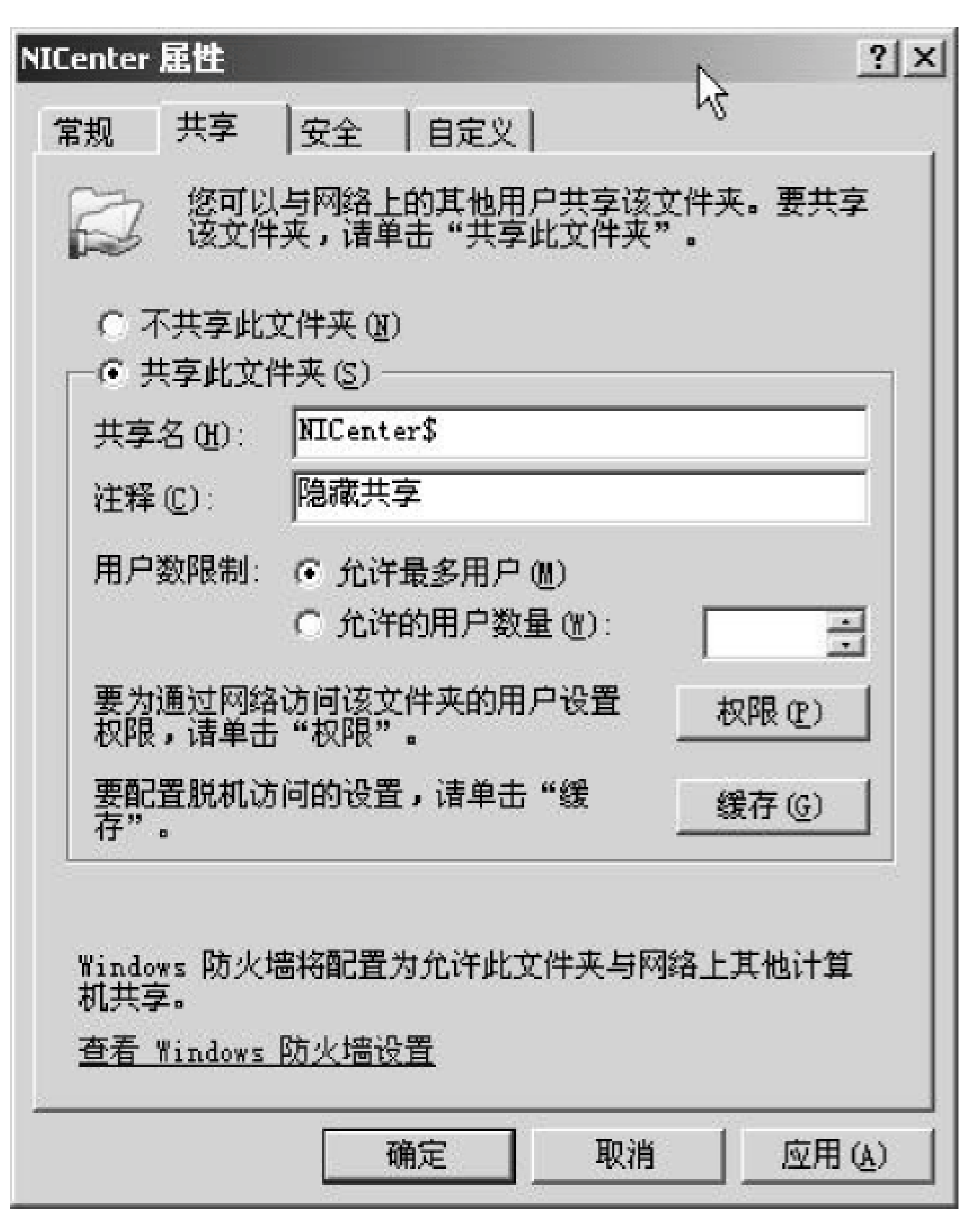


图 7-14　对共享文件夹设置隐藏属性

4）物理形式的入侵信息

物理形式的入侵包括未授权的对网络硬件连接和对物理资源的未授权访问。入侵者会利用各种方法进入用户的网络(一般为内部网络)，然后进行各种非法操作，如安装应用软件、修改系统参数和删除用户数据等。例如，现在不少单位和家庭都安装了无线路由器来提供无线上网服务，但大部分用户对无线路由器的用户接入即没有进行用户认证，也没有进行

加密，而且大部分还打开了 DHCP 服务，只要入侵者的无线网卡设置为“自动获取 IP”地址，就可以通过无线路由器来访问 Internet 或公司的内部网络。

7.3.5 IDS 的信息分析

IDS 对于收集到的各类信息(如系统、网络、数据及用户活动状态和行为等)，一般通过三种技术手段进行分析：模式匹配、统计分析和完整性分析。其中前两种方法用于实时的入侵检测，而完整性分析则用于事后分析。

1. 模式匹配

模式匹配就是将收集到的信息与 IDS 数据库中已知的记录进行比较，从而发现违背安全策略的行为，并将此行为确定为入侵或攻击行为。该过程的实现方法多种多样，例如可以通过简单的字符串的匹配来完成，也可以利用复杂的数学算法来进行。一般来说，一种进攻模式可以用一个过程(如执行一条指令)或一个输出(如获得权限)来表示。

模式匹配的最大优点是只需收集相关的数据集合，系统的负担较小，且技术已相当成熟。IDS 的模式匹配有些类似于病毒防火墙，只要不断升级各类攻击的数据库，就能够实现较高的检测准确率和效率。但是，模式匹配不能检测到从未出现过的攻击或入侵手段。

2. 统计分析

统计分析方法首先给系统对象(如用户、文件、目录和设备等)创建一个统计描述，统计正常使用时的一些测量属性(如访问次数、操作失败次数和延时等)。测量属性的平均值将被用来与网络、系统的行为进行比较，任何观察值在正常值范围之外时，就认为有入侵或攻击发生。例如，对于使用 Windows 2000 Server 或 Windows Server 2003 的企业域用户，可以根据企业内部管理的规定，允许员工在周一至周五的早上 8:00～下午 6:00 登录域控制器来访问企业的内部资源，如图 7-15 和图 7-16 所示。如果在如图 7-12 所示的“事件查看器”窗口中发现有用户在非规定时间频繁地试图登录该域控制器，则可以确定为入侵行为。

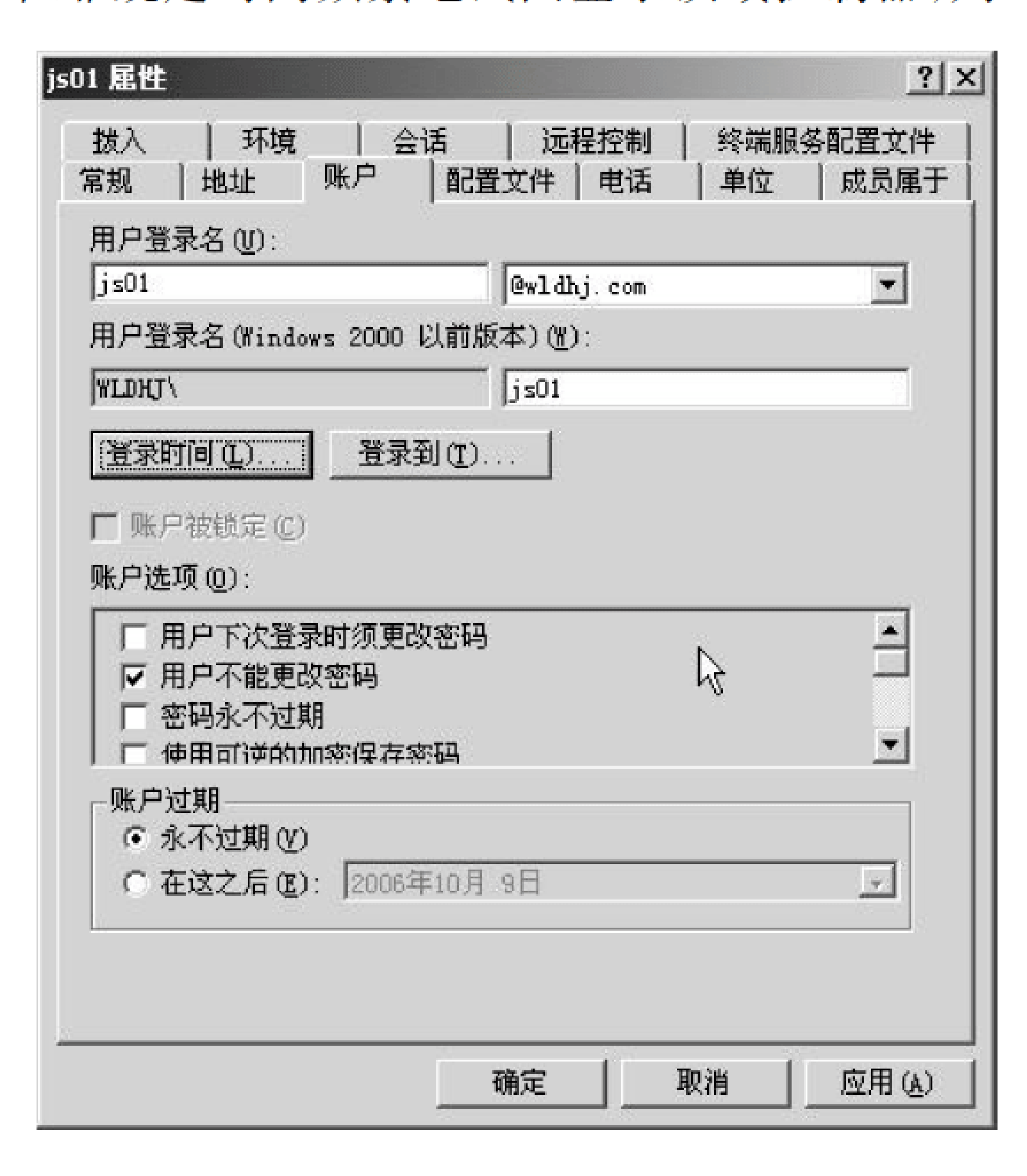


图 7-15　用户账号的属性设置对话框

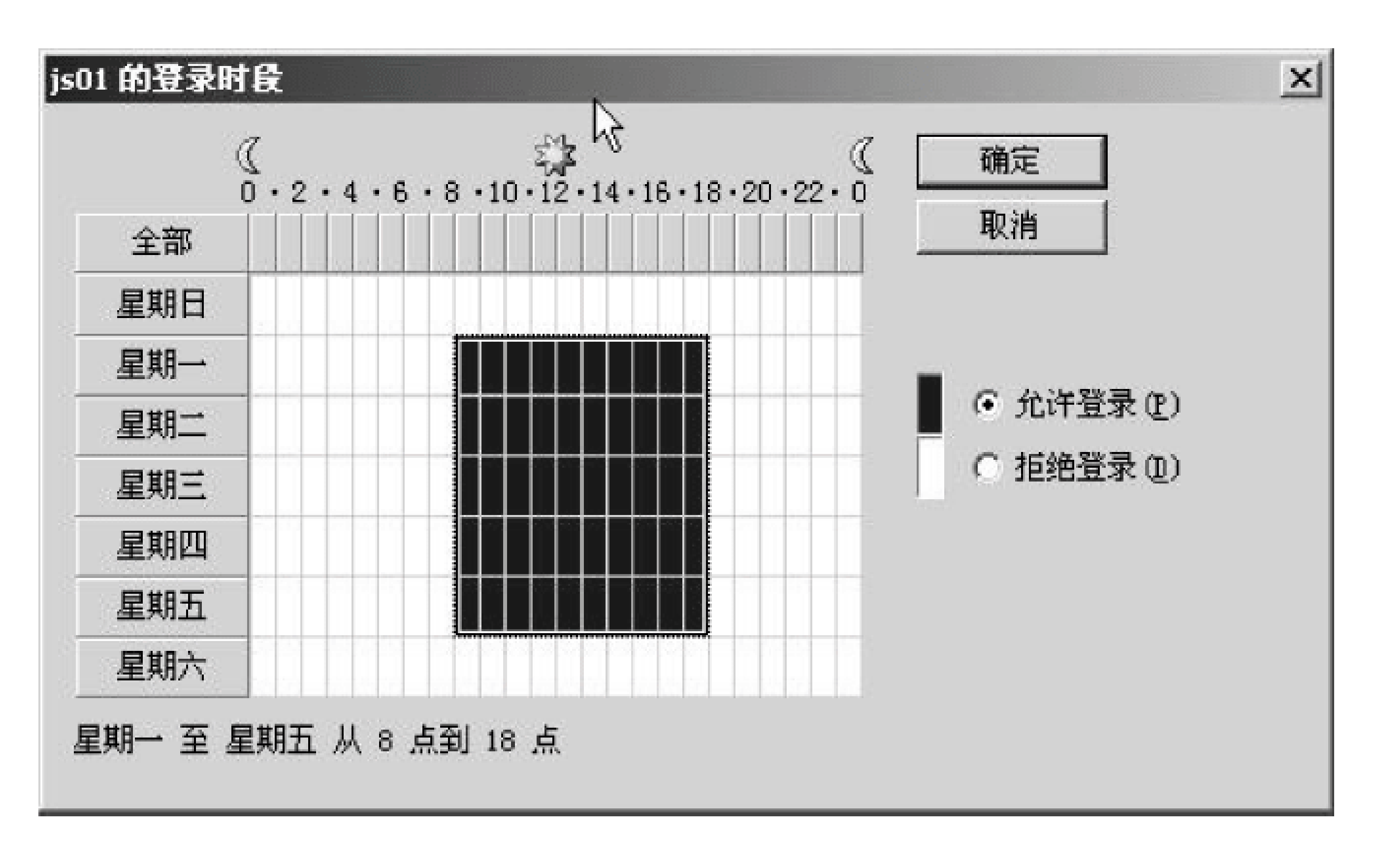


图 7-16 设置用户账号的登录时间

统计分析的优点是可检测到未知的或更为复杂的入侵,缺点是误报、漏报率较高,且不适应用户正常行为的突然改变。

3. 完整性分析

完整性分析主要关注某个文件或对象是否被更改,可以通过该文件或该文件所在目录的属性来发现。完整性分析利用强有力的加密机制,可以识别微小的变化。完整性分析的优点是不管模式匹配方法和统计分析方法能否发现入侵,只要是成功的攻击导致了文件或其他对象的任何改变,它都能够发现。其缺点是一般以批处理方式实现,不用于实时响应。尽管如此,完整性检测方法还应该是网络安全产品的必要手段之一。例如,可以在每一天的某个特定时间内开启完整性分析模块,对网络系统进行全面的扫描检查。

7.3.6 IDS 的特点

入侵检测被认为是继防火墙之后的第二道安全闸门,它在尽量不影响网络性能的情况下对网络进行监测,从而提供对各类攻击和误操作的实时防范。入侵检测是防火墙的有机补充,可帮助系统应对网络攻击和入侵,扩展了系统的安全管理手段(包括安全审计、监视、攻击识别和响应等),提高了信息安全基础结构的完整性。它从计算机网络系统中的多个关键点(如路由器、防火墙和服务器等)收集信息,并分析这些信息,再通过一定的措施查看网络中是否有违反安全策略的行为和遭到袭击的迹象。这些功能都是通过 IDS 执行以下的任务来实现的。

(1) 收集、分析用户及系统的各项活动。

(2) 对系统构造和弱点的审计。

(3) 识别响应已知进攻和入侵的活动模式,并且采取一定的方式通知网络管理人员。

(4) 异常行为模式的统计分析。

(5) 评估重要系统和数据文件的完整性。

(6) 操作系统的审计跟踪管理,并识别用户违反安全策略的行为。

对一个成熟的 IDS 来讲,它不但可使系统管理员时刻了解网络系统(包括程序、文件和硬件设备等)的任何变更,还能给网络安全策略的制订提供帮助和指南。更为重要的一点是,它的配置、使用和管理应用简单明了,适应大量的非专业人员使用。另外,入侵检测的规模还应根据网络所受到的威胁、系统构造和用户的安全需求的改变而适时地进行改变。同

时，IDS 在发现入侵后，能够及时作出响应，包括切断网络连接、记录事件和报警等。

7.3.7 IDS 部署实例分析

根据 IDS 信息收集方式的不同，目前的 IDS 产品也基本上分为基于主机、基于网络和混合型三种类型，其中有些是软件形式(以基于主机的信息收集方式为主)，而有些是软件和专用硬件相结合(以基于网络的信息收集方式为主)。下面分别以 ISS RealSecure 和 Cisco IDS 为例进行介绍。

1. ISS RealSecure 的部署

IDS 的典型代表是 ISS(Internet Security Systems，国际因特网安全系统)的 RealSecure，它是一个自动实时的入侵检测和响应系统，通过监控网络传输并自动检测和响应可疑的行为，在系统受到危害之前截取和响应安全漏洞和内部误用，从而最大程度地为企业网络提供安全保障。RealSecure 在网络中的部署如图 7-17 所示，根据企业网络的特点，可以在每一个网络主干(三层交换机)上安装一个网络传感器(Network Sensor)，然后将通过该主干的流量全部镜像到该网络传感器上，再通过 RealSecure 控制台进行分析。对于小型网络来说，可以仅在中心交换机上安装一个网络传感器即可，如图 7-18 所示。

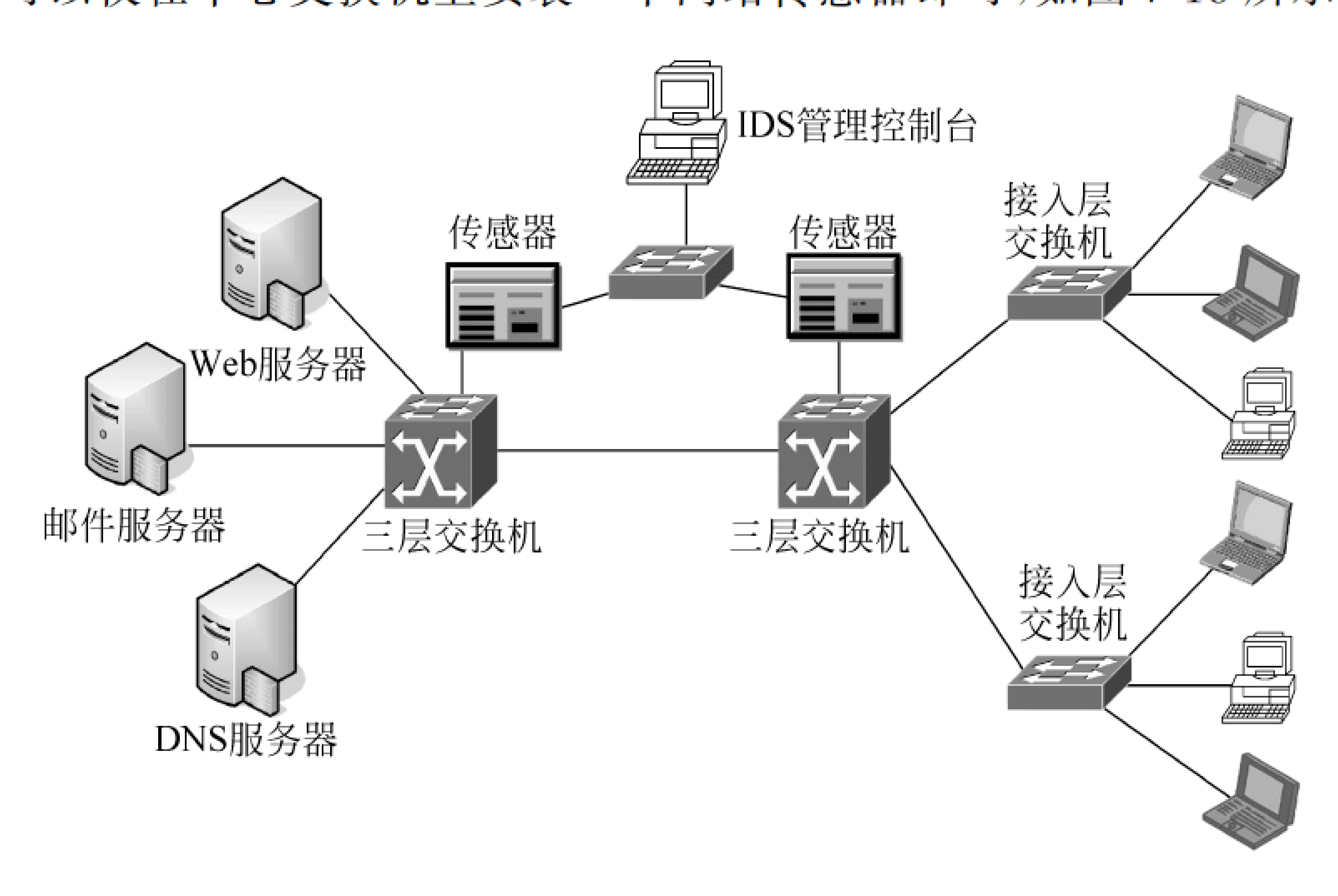


图 7-17　IDS 在大中型网络中的部署

RealSecure 是一种混合型的入侵检测系统，同时提供基于网络和主机的实时入侵检测。其控制台可以运行在 Windows 2000/2003 等操作系统上。RealSecure 的传感器是自治的，能被许多控制台控制。

(1) RealSecure 控制台。可同时对多台网络传感器和服务器代理进行管理；对被管理传感器进行远程的配置和控制；各个监控器发现的安全事件实时地报告到控制台。

(2) Network Sensor。网络传感器，对网络进行监听并自动对可疑行为进行响应，最大程度保护网络安全；运行在特定的主机上(目前广泛使用的 RealSecure 6.x/7.x 可运行在 UNIX、Linux 和 Windows 2000/2003 操作系统上)，监听并解析所有的网络信息，及时发现具有攻击特征的信息包；检测本地网段，查找每一数据包内隐藏的恶意入侵，对发现的入侵做出及时的响应。当检测到攻击时，网络传感器能即刻做出响应，进行报警/通知(向管理控制台报警、向安全管理员发送 E-mail、SNMP trap、查看实时会话和通报其他控制台)，记录

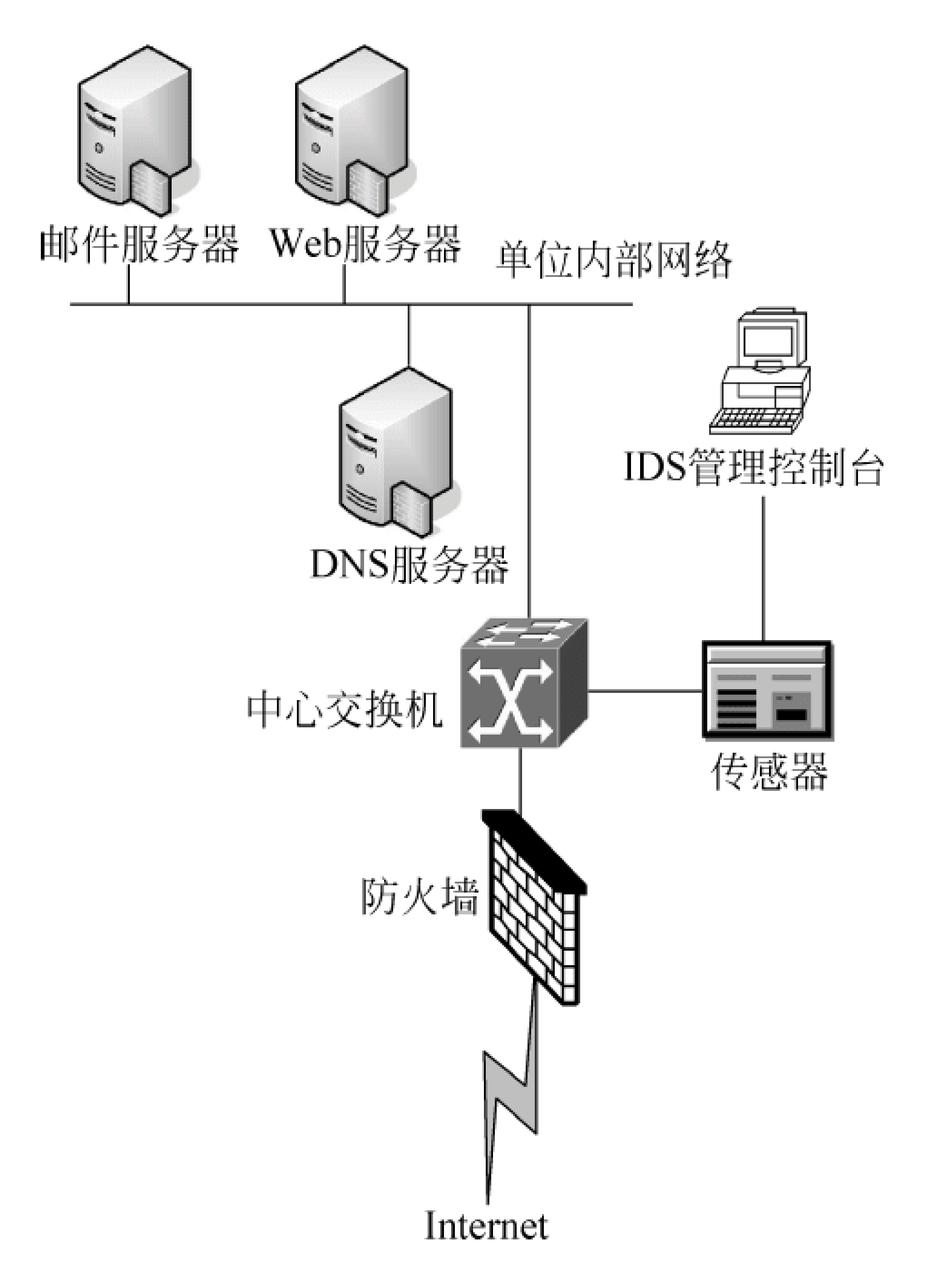


图 7-18 IDS 在小型网络中的部署

现场(记录事件日志及整个会话),采取安全响应行动(终止入侵连接、调整网络设备配置,如防火墙、执行特定的用户响应程序)。

(3) Server Sensor。服务器传感器,它属于一种服务器代理,安装在各个服务器(如图 7-17 和图 7-18 所示的E-mail、Web 和 DNS 服务器等)上,对主机的核心级事件、系统日志及网络活动实现实时入侵检测。具有包拦截、智能报警及阻塞通信的能力,能够在入侵到达操作系统或应用之前主动阻止入侵;自动重新配置网络引擎和选择防火墙阻止黑客的进一步攻击。

2. Cisco IDS 部署

在网络安全领域中,防火墙就好像是坚固的门锁和窗闩,能够阻挡他人的非法入侵。事实上,好的安全战略也应该使用入侵检测。与安全大厦内的警报器和摄像机相似,IDS 警报不但能为警卫提供很多详细信息(包括入侵者进入大厦的方法和目前所在的位置等),还能提供必要的数据,帮助安全管理人员确定快速缉拿入侵者的最佳方式,以及将来怎样预防类似入侵的发生。

Cisco 公司的 IDS 产品多以硬件形式存在,同时 Cisco 公司不但推出专用的 IDS 产品(如 Cisco-IDS-4200 系列),而且还为 Cisco 交换机、路由器和防火墙开发了专门的硬件模块。只要在这些网络设备上安装相应的模块就可以作为一台网络传感器来使用。同时,Cisco 基于主机的代理(Cisco 安全代理)可以运行在服务器主机上,为主机提供安全保障。

更值得一提的是,为了同时管理网络中的大量传感器,Cisco 公司使用了 IDS 管理员中心(IDS MC),它能够在一个管理控制台上同时管理几百个传感器。IDS MC 是 Cisco Works 2000 VPN/安全管理解决方案(VMS)产品的一个组件,可以部署在 Windows 2000 (Service Pack3)及以上版本的操作系统上。

还值得一提的是,在中小型网络中,为了同时监控多个网段,Cisco 公司还推出了多监控接口的传感器,在该传感器上提供了多个网络接口,每一个网络接口可以分别连接一个网

段，如图 7-19 所示。需要说明的是，多监控接口从 Cisco IDS 4.1 版本开始支持。

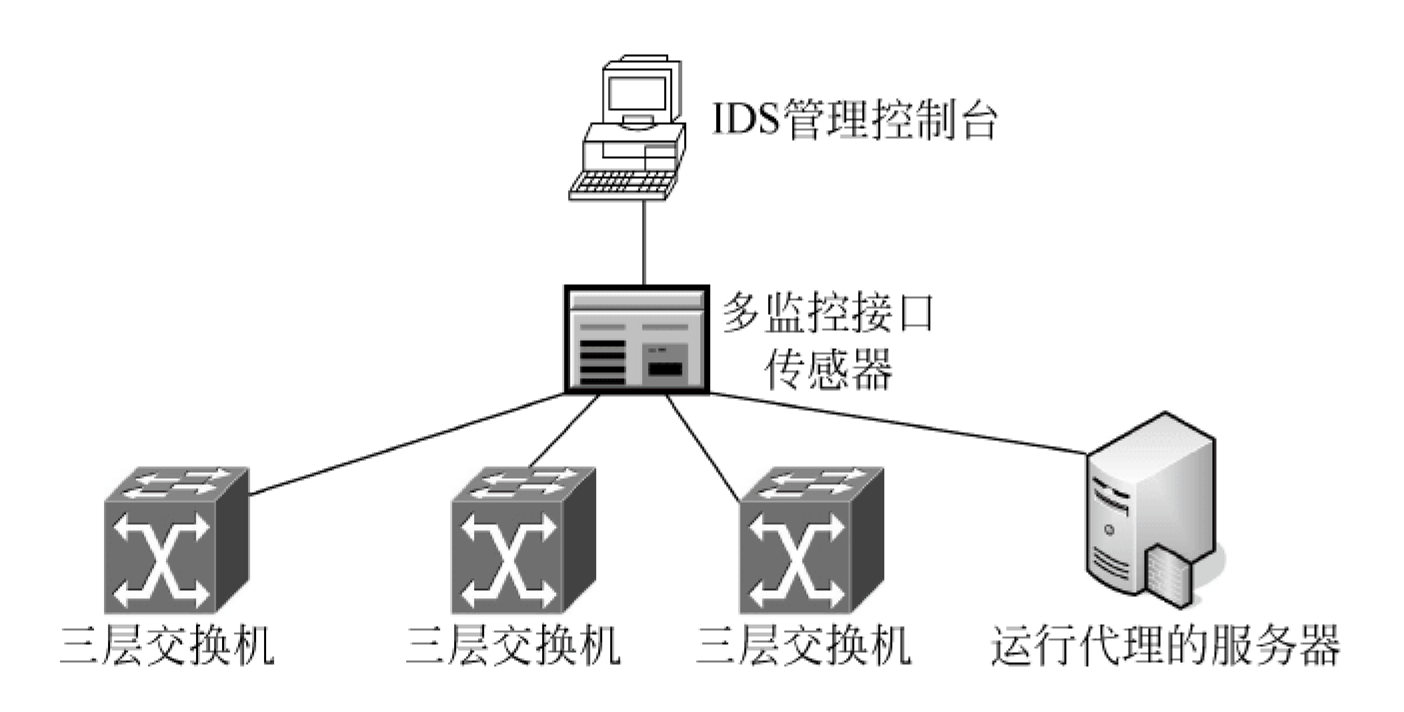


图 7-19　使用多监控接口传感器的 IDS

7.4　IPS 技术及应用

安全防护是一个多层次的保护机制，它既包括网络的安全策略（相关的安全管理制度、系统安全策略的运行等），又包括防火墙、防病毒和入侵检测系统等产品的部署和应用，同时还根据技术的发展，继 IDS 后推出了 IPS（Intrusion Protection System，入侵防御系统）。由此可见，为了保障网络安全，还必须建立一套完整的安全防护体系，进行多层次、多手段的检测和防护。IPS 正是构建安全防护体系不可缺少的一个环节。

7.4.1　IPS 的概念

IPS 是继 IDS 之后发展起来的一项新型技术，它在继承了 IDS 优势的同时，避免了 IDS 存在的一些不足，适应了现代计算机网络对安全的要求。

IPS 是一种主动的、智能的入侵检测和防御系统，其设计目的主要是预先对入侵活动和攻击行为的网络流量进行拦截，避免造成损失。IDS 以关联方式部署在不同的服务器和网段上，先将服务器或网段上的流量镜像到网络传感器上，再通过 IDS 管理控制台进行分析，如果发现入侵或攻击，则会产生报警，IDS 在网络中的部署方式如图 7-20 所示。与 IDS 相比，IPS 最大的不同是以串联的方式部署在网络的进出口处，像防火墙一样，它对进出网络的所有流量进行分析。当检测到有入侵或攻击企图后，会自动将相应的数据包丢弃，或采取相应的措施将攻击源阻断。IPS 在网络中的部署方式如图 7-21 所示。

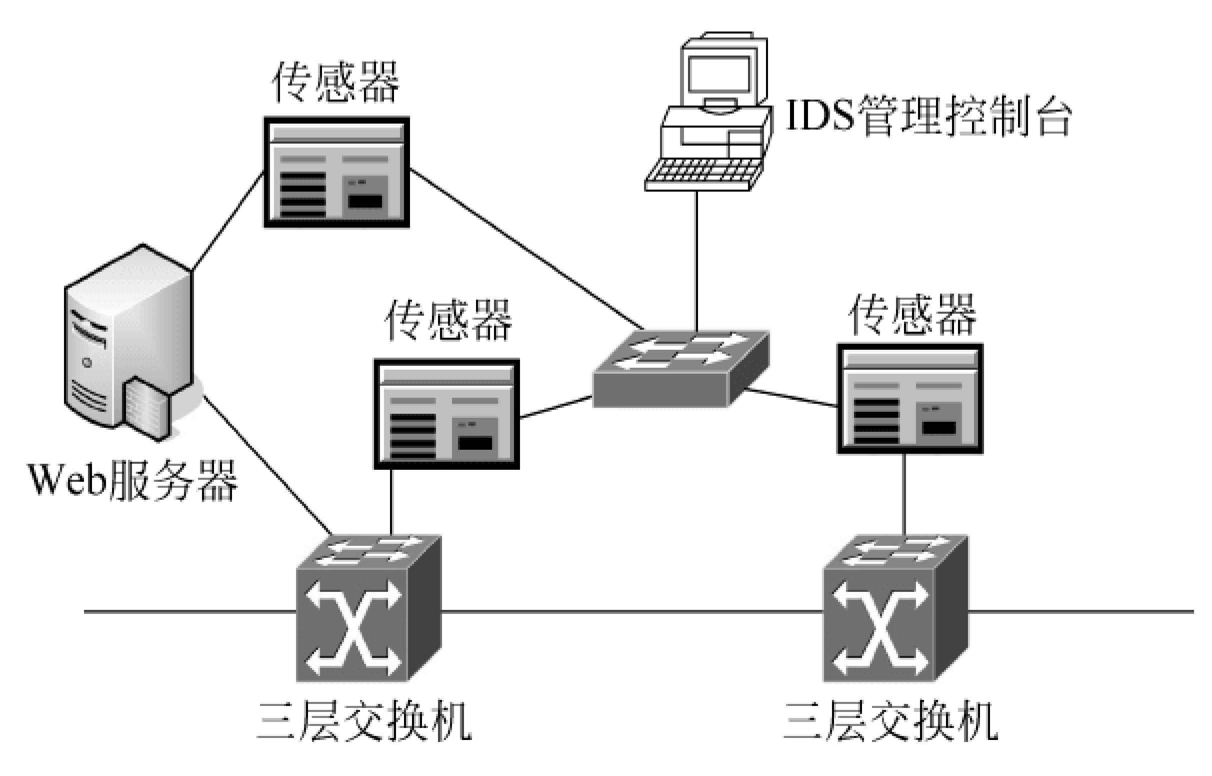


图 7-20　IDS 在网络中的部署方式

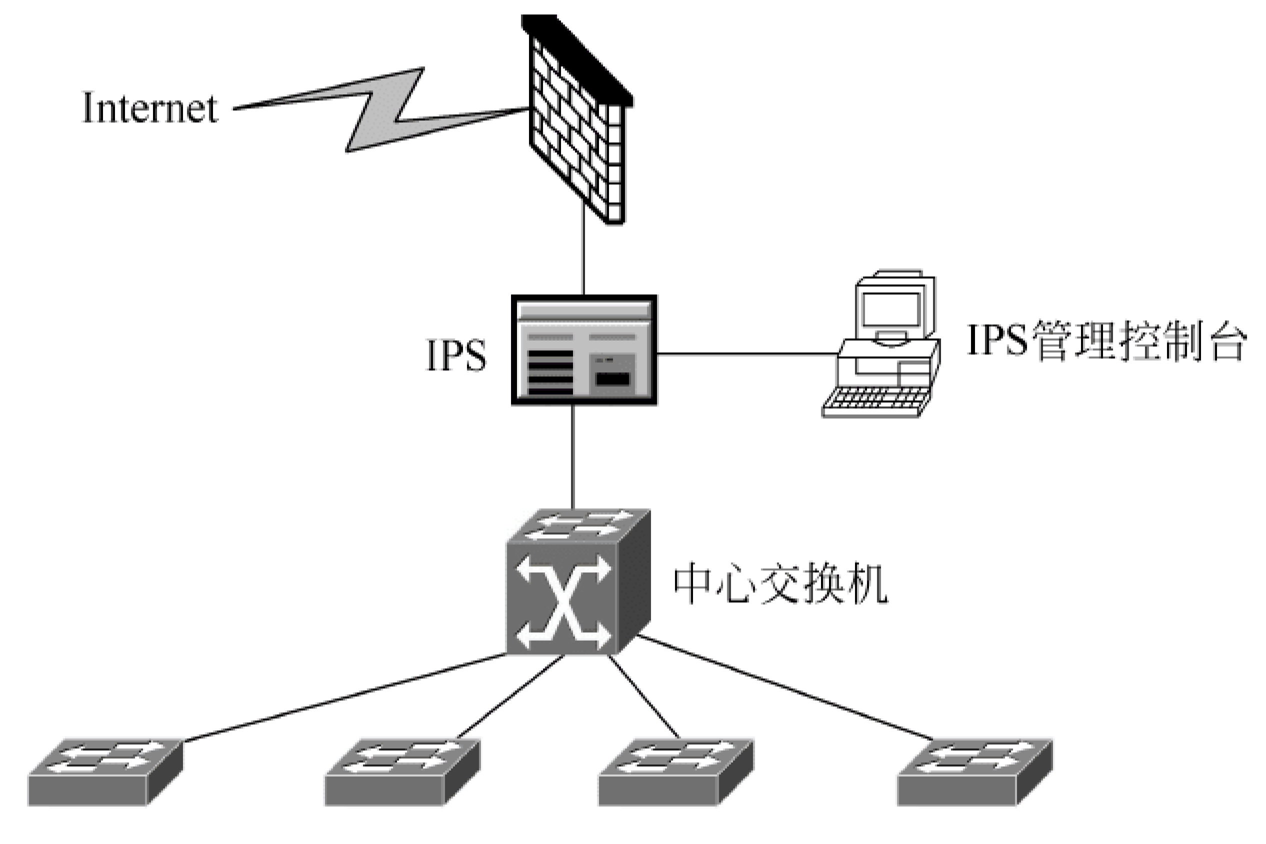


图 7-21　IPS 在网络中的部署方式

在介绍 IPS 时，不得不提到防火墙和 IDS。防火墙是实施访问控制策略的系统，对流经网络的流量进行检查，拦截不符合安全策略的数据包。同时，传统的防火墙只能对 OSI 参考模型第三层（网络层）和第四层（传输层）的数据单元进行检查，不能检测应用层的内容，而且防火墙的包过滤技术不会针对每一个字节进行检查，因而也就无法发现攻击活动。所以，防火墙的主要功能是拒绝那些明显可疑的网络流量，但仍然允许某些流量通过，因此防火墙对于大部分入侵攻击仍然无能为力。

IDS 通过监视网络或系统资源，寻找违反安全策略的行为或攻击迹象，并发出报警。IDS 从工作方式来看基本上是被动的，在攻击或入侵实际发生之前，IDS 往往无法预先发出报警。而 IPS 则倾向于提供主动防御，其设计目的是预先对入侵活动和攻击性网络流量进行拦截，避免其造成损失，而不像 IDS 那样简单地在恶意流量传送时或传送后才发出警报。IPS 是通过直接嵌入到网络流量中实现这一功能，即通过一个网络端口接收来自外部系统的流量，经过检查确认其中不包含异常活动或可疑内容后，再通过另外一个端口传送到内部系统中。这样一来，有问题的数据包，以及所有来自同一数据流的后续数据包，都能在 IPS 设备中被清除掉。

IPS 实现实时检查和阻止入侵的原理在于 IPS 拥有数目众多的过滤器，能够防止各种攻击。当新的攻击手段被发现之后，IPS 就会创建一个新的过滤器。所有流经 IPS 的数据包都被分类，分类的依据是数据包的头部信息，如源 IP 地址、目的 IP 地址、端口号和应用域等。每种过滤器负责分析相对应的数据包。通过检查的数据包可以继续往前发送，包含恶意内容的数据包就会被丢弃，被怀疑的数据包需要接受进一步的检查。

IPS 应具有以下的技术特征。

（1）嵌入式运行。只有以嵌入模式运行的 IPS 设备才能够实现实时的安全防护，实时阻断所有可疑的数据包，并对该数据流的剩余部分进行拦截。

（2）深入分析和控制。IPS 必须具有深入分析能力，以确定哪些流量已经被拦截，并能够根据攻击类型、策略等来确定哪些流量应该被拦截。

（3）入侵特征库。与防病毒系统的病毒库一样，较为完整的高质量的入侵特征库是 IPS 高效运行的必要条件。当选择一款 IPS 产品时，除考虑其硬件性能和所采用的技术等指标外，还要重点考虑 IPS 入侵特征库的升级等问题。

（4）高效处理能力。IPS 必须具有对数据包的高效处理能力，争取对整个网络性能的

影响降至最低水平，避免 IPS 成为网络的瓶颈。

7.4.2 IPS 的分类

IPS 根据部署方式的不同，分为基于主机的入侵防御系统(Host IPS，HIPS)、基于网络的入侵防御系统(Network IPS，NIPS)和应用入侵保护(Application Intrusion Prevention，AIP)三种类型。

1. 基于主机的入侵防御

基于主机的入侵防御通过在服务器等主机上安装代理程序来防止对主机的入侵和攻击，保护服务器免受外部入侵或攻击。HIPS 可以根据自定义的安全策略及分析学习机制来阻断对服务器等主机发起的恶意入侵，HIPS 可以阻断缓冲区溢出、更改登录口令、改写动态链接库，以及其他试图获得操作系统入侵权的行为，加强了系统整体的安全性。

HIPS 利用由包过滤、状态包检测和实时入侵检测组成的分层防护体系，不但能够阻止诸如缓冲区溢出这一类的已知攻击，还能够防范未知攻击，防止针对 Web 页面、应用系统和资源的未授权的任何非法访问，提供对主机整体的保护。它能够在满足网络实际吞吐率的前提下，最大限度地保护主机的敏感内容，既可以将相关软件嵌入到应用程序对操作系统的调用中，来拦截针对操作系统的可疑调用，提供对主机的安全防护，也可以更改操作系统内核程序的方式，提供比操作系统更加严谨的安全控制机制。HIPS 与具体的主机或服务器上所运行的操作系统紧密相关，不同的操作系统需要不同的代理程序。

2. 基于网络的入侵防御

基于网络的入侵防御通过检测流经的网络流量，提供对网络系统的安全保护。与 IDS 的并联方式不同，由于 IPS 采用串联方式，所以一旦检测出入侵行为或攻击数据流，NIPS 就可以去除整个网络会话。另外，由于 IPS 以串联方式接入整个网络的进出口处，所以 NIPS 的性能也影响整体网络的性能，NIPS 有可能成为整个网络的瓶颈。为此，对 NIPS 的硬件组成和处理能力就提出了更高的要求。

除在硬件上为 NIPS 提供保障外，还需要从实现技术上寻找突破。NIPS 吸取了目前几乎 IDS 所有的成熟技术，包括特征匹配、协议分析和异常检测等。其中，特征匹配具有准确率高、速度快等特点，是应用最为广泛的一项技术。基于状态的特征匹配不但检测攻击行为的特征，还要检查当前网络的会话状态，避免受到欺骗攻击。协议分析是一种较新的入侵检测技术，它充分利用网络协议的特征，并结合高速数据包捕捉和协议分析技术，来快速检测某种攻击特征。协议分析能够理解不同协议的工作原理，以此分析这些协议的数据包，来寻找可疑或不正常的访问行为。

3. 应用入侵防护

应用入侵防护是 NIPS 产品的一个特例，它把 NIPS 扩展成为位于应用服务器之前的网络设备，为应用服务器提供更安全的保护。AIP 被设计成一种高性能的设备，配置在特定的网络链路上，以确保用户遵守已设定好的安全策略，保护服务器的安全。而 NIPS 工作在网络上，直接对数据包进行检测和阻断，与具体的服务器或主机的操作系统平台无关。

7.4.3 IPS 的发展

IDS 入侵检测系统一直以来充当了安全防护系统的重要角色。IDS 技术是通过从网络上获取数据包后进行分析，从而检测和识别出系统中的未授权或异常现象。IDS 注重的是

网络监控、审核跟踪，告知网络是否安全，发现异常行为时，自身不作为，而是通过与防火墙等安全设备联动的方式进行防护。目前，IDS是一种受到企业欢迎的解决方案，但其存在以下几个显著缺陷：部署过程复杂、误报率高及自身防攻击能力较差等。

以上现象的存在，是因为绝大多数IDS系统都是被动的，而不是主动性的。在攻击实际发生之前，IDS往往无法预先发出报警。IPS则倾向于提供主动性的防护，其设计目的为预先对入侵活动和攻击性网络流量进行拦截，避免其造成损失，而不是简单地在恶意流量传送时或传送后才发出报警。目前，集病毒、木马、入侵和攻击等为一体的混合威胁不断发展，所以单一的防御措施已经无能为力，企业需要对网络进行多层、深层的防护来有效保证其网络安全。真正的深层防护体系不仅能够发现恶意代码，而且还能够主动地阻止恶意代码的攻击。在当前混合威胁泛滥的情况下，只有深层防御才可以确保网络的安全。IPS在深层防御保护方面具有一定的技术优势。

但是有专家认为，入侵防护应该是由多种安全设备组成的安全体系共同来实现，而不是由IPS单独来完成，IPS只是主动防御的一部分，而不是主动防御的全部。主动防御系统还需要加入应用级防火墙与应用级IDS，应用级的IDS产品能够重组信息流，跟踪应用会话过程，并准确描述和识别攻击；而应用级的防火墙能够阻断向应用层发起的攻击，保护Web应用。

所以，从较长的一段时间来看，IPS还不可能完全取代IDS和防火墙产品，IPS还有许多不够完善的地方，如单点故障、性能瓶颈、误报和漏报等。这是由于IPS必须串联到网络中，这就可能造成网络瓶颈或单点故障。如果IDS出现故障，最坏的情况也就是造成某些攻击无法被检测到；而串联式的IPS设备出现问题，就会严重影响网络的正常运转，甚至造成所有用户都将无法访问企业网络提供的服务。即使正常使用的IPS设备也仍然是一个潜在的网络瓶颈，串联到网络中的IPS不仅会增加正常的响应时间，而且会降低网络的效率，IPS必须与数千兆或者更大容量的网络流量保持同步，尤其是当加载了数量庞大的检测特征库时，设计不够完善的IPS设备将很难支持这种响应速度，这就为IPS设备的制造技术和成本提出了更高的要求。

针对以上问题，IPS厂商纷纷采用各种方式加以解决。例如，综合应用多种检测技术，采用专用硬件加速系统来提高IPS的运行效率等。不过，需要说明的是，因为网络威胁的多样性和综合性已越来越突出，所以IPS的不足并不会成为阻止人们使用IPS的理由。在众多的安全产品中，入侵防御系统的重要性会不断被用户所认可。

由于IPS技术还处于快速的发展阶段，相应的网络应用目前还较少。为此，本章仅介绍了IPS的相关概念和技术优势，对IPS感兴趣的读者可关注其发展。

习　题

7-1　什么是网络攻击？网络攻击主要采取哪些方式？

7-2　名词解释：死亡之Ping、泪滴攻击、ICMP泛洪、UDP泛洪、Land攻击、Smurf攻击、电子邮件炸弹、口令攻击、缓冲区溢出。

7-3　什么是扫描技术？区分端口扫描和漏洞扫描的不同之处。

7-4　介绍假消息攻击的特点及常见的实现方法。

7-5　分别介绍脚本攻击和 ActiveX 攻击的特点及实现方法。

7-6　分别介绍 DoS 和 DDoS 攻击的实现方法和特点。

7-7　名词解释：IDS、误报、漏报。

7-8　试分析 IDS 的异常检测、滥用检测和混合检测三种模型的原理与应用特点。

7-9　结合实际，说明 IDS 中数据的收集和分析方法及重要性。

7-10　与 IDS 相比，IPS 具有哪些功能优势？

7-11　联系网络安全实际，试分析 HIPS、NIPS 和 AIP 的技术特点和应用优势。

第8章 防火墙技术及应用

网络防火墙(简称为“防火墙”)是计算机网络安全管理中应用最早和技术发展最快的安全产品之一。随着以 Internet 为主的计算机网络应用的迅猛发展,各种安全问题和安全隐患日渐突出。防火墙则需要关注网络应用实际,最大可能地解决各类安全问题,堵塞已知的安全漏洞,为用户提供可信赖的网络应用区域。目前,防火墙技术已不再仅仅局限于单一的防火墙产品,同时已集成到操作系统、杀病毒软件、路由器和交换机等各类网络产品中。为此,本章将立足用户的安全需要,侧重于对防火墙技术和应用的介绍,而不是仅仅关注某一类防火墙产品,从而开阔读者的知识面,培养读者分析和解决网络安全问题的能力。

8.1 防火墙技术概述

防火墙的产生动因之一是防范非法用户的入侵,为主机或局域网提供安全防护。目前,防火墙已成为大多数机构构建可信赖安全网络的主要支柱。

8.1.1 防火墙的概念

护城河是古人在防御手段上利用水的作用,引水注入人工开挖的壕沟,形成人工河作为城墙或重要建筑的屏障,一方面维护城内治安,另一方面阻止入侵者的进入。在早期修建木质结构房屋时,为防止火灾的发生和蔓延,建设者将坚固的石块堆砌在房屋周围作为屏障,这种用石块构筑的屏障称为“防火墙”。

计算机网络中的防火墙功能类似于古代的护城河和建筑物周围的石块屏障。从网络的结构来看,当一个局域网接入互联网(如 Internet)时,局域网内部的用户就可以访问互联网上的资源,同时外部用户也可以访问局域网内的主机资源。然而,在许多情况下,局域网属于单位的内部网络,有一些资源是不允许外网用户来访问的。为此,需要在局域网与互联网之间构建一道安全屏障,其作用是阻断来自外部网络对局域网的威胁和入侵,为局域网提供一道安全和审计的关卡。

防火墙是指设置在不同网络(如可信赖的企业内部局域网和不可信赖的公共网络)之间或网络安全域之间的一系列部件的组合,通过监测、限制、更改进入不同网络或不同安全域的数据流,尽可能地对外部屏蔽网络内部的信息、结构和运行状况,以防止发生不可预测的、潜在破坏性的入侵,实现网络的安全保护。防火墙从功能上来说,是被保护的内部网络与外部网络之间的一道屏障,是不同网络或网络安全域之间信息的唯一出入口,能根据内部网络用户的安全策略控制(允许、拒绝、监测)出入网络的信息流;防火墙从逻辑上来说,是一个分离器,一个限制器,也是一个分析器,能够有效地监控内部网和外部网络(如 Internet)之

间的所有活动,保证了内部网络的安全;从物理实现上来说,防火墙是位于网络特殊位置的一系列安全部件的组合,它既可以是专用的防火墙硬件设备,也可以是路由器或交换机上的安全组件,还可以是运行有安全软件的主机。

防火墙本身应具有较强的抗攻击能力,能够提供信息安全服务。防火墙是实现网络和信息安全的基础设施,一个高效可靠的防火墙应具备以下的基本特性。

(1) 防火墙是不同网络之间,或网络的不同安全域之间的唯一出入口,从里到外和从外到里的所有信息都必须通过防火墙。

(2) 通过安全策略来控制不同网络或网络不同安全域之间的通信,只有本地安全策略授权的通信才允许通过。

(3) 防火墙本身是免疫的,即防火墙本身具有较强的抗攻击能力。

8.1.2 防火墙的基本功能

防火墙技术随着计算机网络技术的发展而不断向前发展,其功能也越来越完善。一台高效可靠的防火墙应具有以下的基本功能。

1. 监控并限制访问

针对网络入侵的不安全因素,防火墙通过采取控制进出内、外网络数据包的方法,实时监控网络上数据包的状态,并对这些状态加以分析和处理,及时发现存在的异常行为。同时,根据不同情况采取相应的防范措施,从而提高系统的抗攻击能力。

2. 控制协议和服务

针对网络自身存在的不安全因素,防火墙对相关协议和服务进行控制,使得只有授权的协议和服务才可以通过防火墙,从而大大降低了因某种服务、协议的漏洞而引起安全事故的可能性。例如,当允许外部网络用户匿名访问内部 Web 服务器时,就需要在防火墙上对访问协议和服务进行限制,只允许 http 协议利用 TCP 80 端口进入网络,而其他协议和端口将被拒绝。防火墙可以根据用户的需要在向外部用户开放某些服务(如 WWW、FTP 等)的同时,禁止外部用户对受保护的内部网络资源进行访问。

3. 保护内部网络

针对应用软件及操作系统的漏洞或“后门”,防火墙采用了与受保护网络的操作系统、应用软件无关的体系结构,其自身建立在安全操作系统之上。同时,针对受保护的内部网络,防火墙能够及时发现系统中存在的漏洞,对访问进行限制;防火墙还可以屏蔽受保护网络的相关信息。

4. 网络地址转换

网络地址转换(Network Address Translation,NAT)是指在局域网内部使用私有 IP 地址,而当内部用户要与外部网络(如 Internet)进行通信时,就在网络出口处将私有 IP 地址替换成公用 IP 地址。NAT 具有以下主要功能。

(1) 缓解目前 IP 地址(主要是 IPv4)紧缺的局面。一个单位可以申请有限的几个甚至是一个合法的公用 IP 地址,通过 NAT 就可以实现使用私有 IP 地址的内部局域网用户访问 Internet。

(2) 屏蔽内部网络的结构和信息。一个单位如果不希望外部网络用户知道本单位内部的网络结构时,可以通过 NAT 将内部网络与外部网络隔离开来,即使外部用户能够访问单

位内部的部分网络服务(如 WWW、FTP 和电子邮件等),也感觉不到是通过 NAT 进行 IP 地址转换的。同时,所有内部网络中的计算机对于外部网络来说是不可见的,而位于内部网络中的计算机用户通常也不会意识到 NAT 的存在。

(3) 保证内部网络的稳定性。如果内部网络更换了 ISP,意味着要更换公用 IP 地址。使用了 NAT 后,只需要在 NAT 设备(如防火墙、路由器等)上进行简单的设置即可,单位内部的计算机和网络设备不需要进行任何改动。

(4) 适应目前国内互联网络的应用现状。目前,国内互联网络之间存在的互联互通问题已非常明显,许多高校和企业在网络出口处都提供了两条以上的线路,每一条线路连接一个 ISP,如中国电信、中国网通、中国联通、中国教育和科研网等。

通过 NAT,解决了同一内部网络使用多出口的问题。目前,NAT 主要通过防火墙和路由器来实现。

5. 虚拟专用网

虚拟专用网(Virtual Private Network,VPN)是在公用网络中建立的专用数据通信网络。在虚拟专用网中,任意两个节点之间(如局域网与局域网之间、主机与主机之间、主机与局域网之间)的连接并没有传统专用网络所需的端到端的物理链路,而是利用已有的公用网络资源(如 Internet、ATM 和帧中继等)建立的逻辑网络,节点之间的数据在逻辑链路中传输。虚拟专用网中的"虚拟"是指用户不需要拥有实际的长途数据线路,而是使用 Internet 等公用数据网络的长途数据线路;"专用网"是指用户可以为自己制定一个符合自己需求的网络。目前 VPN 在网络中得到了广泛应用,作为网络特殊位置的防火墙应具有 VPN 的功能,以简化网络配置和管理。有关 VPN 的详细内容将在本章第 9 章进行专门介绍。

6. 日志记录与审计

当防火墙系统被配置为所有内部网络与外部网络(如 Internet)连接均需经过的安全节点时,防火墙会对所有的网络请求做出日志记录。日志是对一些可能的攻击行为进行分析和防范的十分重要的情报信息。另外,防火墙也能够对正常的网络使用情况做出统计。这样网络管理人员通过对统计结果的分析,就能够掌握网络的运行状态,进而更加有效地管理整个网络。

8.1.3 防火墙的基本原理

所有防火墙功能的实现都依赖于对通过防火墙的数据包的相关信息进行检查,而且检查的项目越多、层次越深,则防火墙越安全。由于现在计算机网络结构采用自顶向下的分层模型,而分层的主要依据是各层的功能划分,不同层次功能的实现又是通过相关的协议来实现的。所以,防火墙检查的重点是网络协议及采用相关协议封装的数据。

对于一台防火墙来说,如果知道了其运行在 OSI 参考模型的哪一层,就可以知道它的体系结构是什么,主要的功能是什么。例如,当防火墙主要工作在 OSI 参考模型的网络层时,由于网络层的数据是 IP 分组,所以防火墙主要针对 IP 分组进行安全检查,这时读者需要结合 IP 分组的结构(如源 IP 地址、目的 IP 地址等)来掌握防火墙的功能,进而有针对性地在网络中部署防火墙产品。再如,当防火墙主要工作在应用层时,读者就需要根据应用层的不同协议(如 http、DNS、SMTP、FTP 和 Telnet 等)来了解防火墙的主要功能。

一般来说,防火墙在 OSI 参考模型中的位置越高,防火墙需要检查的内容就越多,对

CPU 和内存的要求就越高，也就越安全。但是，防火墙的安全不是绝对的，它寻求一种在可信赖和性能之间的平衡。在防火墙的体系结构中，在 CPU 和内存等硬件配置基本相同的情况下，高安全性的防火墙的效率和速率较低，而高速度和高效率的防火墙其安全性则较差。为此，对于防火墙的应用业界的共识是：性能和安全之间是成反比的。近年来，随着计算机性能的上升，以及操作系统对对称多处理器（Symmetrical Multi-Processing，SMP）系统及多核 CPU 的支持，防火墙的处理能力得到了加强，防火墙对数据包的处理速度和效率得到了提升，防火墙在 OSI 参考模型中的不同工作位置对其速度和效率的影响逐渐缩小。

8.1.4 防火墙的基本准则

作为可信赖的单位内部网络与不可信赖的外部网络之间的连接节点，防火墙在安全功能上可以遵循以下的基本准则。

1. 所有未被允许的就是禁止的

这一准则是指根据用户的安全管理策略，所有未被允许的通信禁止通过防火墙。基于该准则，防火墙应封锁所有信息流，然后对希望提供的服务逐项开放，对不安全的服务或可能存在安全隐患的服务一律关闭。这是一种非常有效、实用的方法，可以构建一个较为安全的网络应用环境，因为只有经过管理人员确认是安全的服务才被允许使用。

这一准则的优势是安全性高，但弊端是用户所能使用的服务范围受到限制，造成用户使用不方便。例如，Cisco PIX 防火墙的初始化配置就采用了该准则。

2. 所有未被禁止的就是允许的

这一准则是指根据用户的安全管理策略，防火墙转发所有信息流，允许所有的用户和站点对内部网络的访问，然后网络管理员按照 IP 地址等参数对未授权的用户或不信任的站点进行逐项屏蔽。这种方法构成了一种更为灵活的应用环境，可为用户提供更多的服务。其弊端是随着网络服务的增多，网络管理人员的工作量将会随之增大，特别是受保护的网络范围增大时，很难提供可靠的安全防护。目前，许多国产防火墙都使用这一准则。

8.2 防火墙的应用

在计算机网络管理中，防火墙是一种非常有效的安全解决方案，它可以为用户提供一个相对安全的网络环境。但是，并不是说防火墙在安全管理中是万能的，采用了防火墙的网络同样存在一些安全漏洞和隐患。

8.2.1 防火墙在网络中的位置

防火墙多应用于一个局域网的出口处（如图 8-1（a）所示）或置于两个网络中间（如图 8-1（b）所示）。对于绝大多数局域网来说，在将局域网接入 Internet 时，在路由器与局域网中心交换机之间一般都要配置一台防火墙，以实现对局域网内部资源的安全保护。

根据应用的不同，防火墙一般可以分为路由模式防火墙和透明模式防火墙两类。其中，路由模式防火墙可以让处于不同网段的计算机通过路由转发的方式互相通信（如图 8-1（b）所示）。路由模式防火墙存在以下两个局限。

局域网中心交换机
局域网(Intranet)
外部网络(Internet)
路由器
防火墙

(a) 位于局域网出口处的防火墙

防火墙
局域网
局域网

(b) 置于两个局域网中间的防火墙

图 8-1　防火墙在网络中的位置

(1) 防火墙各端口所连接的网络必须位于不同的网段，否则两个网络之间将无法进行通信。

(2) 与防火墙直接连接的设备(计算机、路由器或交换机)的网关都要指向防火墙。

简单地讲，路由模式防火墙是让防火墙同时承担路由器的功能，而路由器主要用于连接不同的网络。

路由模式防火墙也称为"不透明"的防火墙。而透明模式防火墙克服了路由模式防火墙的不足，可以连接两个位于同一逻辑网段的物理子网，将其加入一个已有的网络时可以不用修改边缘网络设备的设置。透明模式防火墙的应用如图 8-1(a)所示。

为了适应不同网络的应用需要，目前市面上的主流防火墙一般都同时支持路由模式和透明模式两种工作模式，使用者可以根据实际的网络需要在两种模式之间进行选择。

8.2.2　使用了防火墙后的网络组成

防火墙是构建可信赖网络域的安全产品。如图 8-2 所示，当一个网络在加入了防火墙后，防火墙将成为不同安全域之间的一个屏障，原来具有相同安全等级的主机或区域将会因为防火墙的介入而发生变化，主要如下所示。

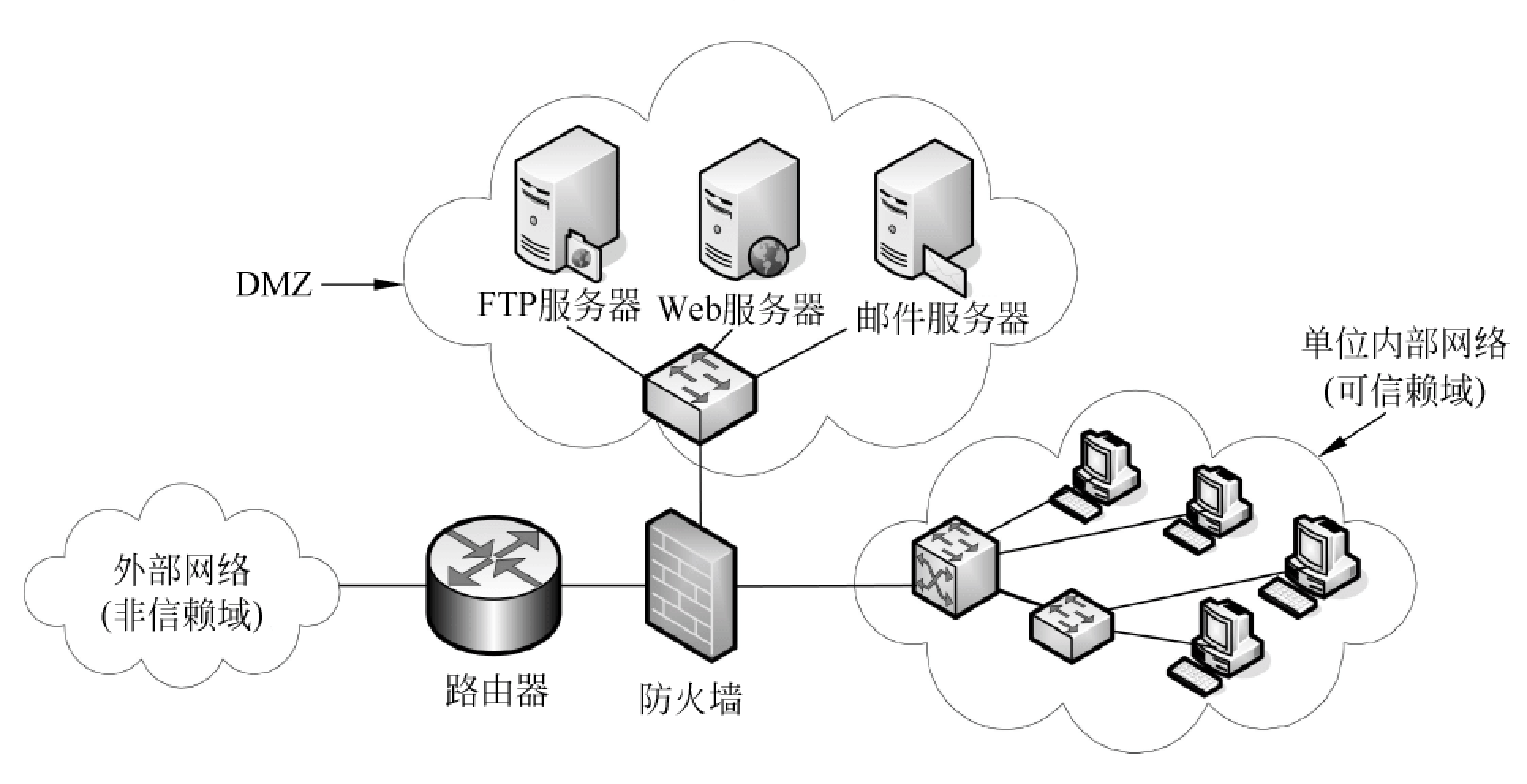


图 8-2　使用防火墙后的网络组成

1. 信赖域和非信赖域

当局域网通过防火墙接入公共网络时，以防火墙为节点将网络分为内、外两部分，其中内部的局域网称为信赖域，而外部的公共网络（如 Internet）称为非信赖域。

2. 信赖主机和非信赖主机

位于信赖域中的主机因为具有较高的安全性，所以称为信赖主机；而位于非信赖域中的主机因为安全性较低，所以称为非信赖主机。

3. DMZ

DMZ(Demilitarized zone)称为“隔离区”或“非军事化区”，它是介于信赖域和非信赖域之间的一个安全区域。因为在设置了防火墙后，位于非信赖域中的主机是无法直接访问信赖区主机的，但原来（未设置防火墙时）位于局域网中的部分服务器（如单位的 Web 服务器、FTP 服务器和邮件服务器等）需要同时向内外用户提供服务。为了解决设置防火墙后外部网络不能访问内部网络服务器的问题，便采用了一个信赖域与非信赖域之间的缓冲区。这个缓冲区中的主机（一般为服务器）虽然位于单位内部网络，但允许外部网络访问。

支持 DMZ 功能的防火墙至少需要提供三个网络接口，一个连接可信赖域，另一个连接非信赖域，还有一个连接 DMZ，如图 8-3 所示。其实，图 8-2 中的非信赖域还包括路由器。在进行 IP 地址分配时，连接可信赖域的接口一般配置内部网络使用的私有 IP 地址，连接非信赖域和 DMZ 的接口一般配置公网 IP 地址。另外，DMZ 接口也可以配置成为私有 IP 地址，然后再通过防火墙或路由器中的 NAT 功能将其映射为一个公网 IP 地址。



图 8-3　防火墙上的网络连接接口

例如，Cisco PIX 防火墙就通过 0～100 之间的安全级别来定义接口的安全类型。在默认配置中，连接非信赖外部网络的接口安全级别为 0，而连接可信赖的内部网络的接口安全级别为 100，DMZ 接口的安全级别可由网络管理员在 1～99 之间选择，一般设置为 50。

8.2.3　防火墙应用的局限性

防火墙虽然是目前应用最为广泛，同时也是最有效的网络安全技术，但是，防火墙并不是全能的，它存在一定的应用局限性，主要表现如下。

1. 防火墙不能防范未通过自身的网络连接

防火墙一般位于内部网络与外部网络的边界处，负责检查所有通过它的通信情况。对于有线网络来说，防火墙是进出网络的唯一节点。但是如果使用无线网络（如无线局域网），内部用户与外部网络之间，以及外部用户与内部网络之间的通信就会绕过防火墙，这时防火墙就没有任何用处。

目前，无线局域网技术的发展非常迅速，应用需求迅速上升。所以，在使用无线网络的环境中必须考虑到防火墙存在的局限性，需要通过其他的安全技术和措施加强对无线网络的安全管理。

2. 防火墙不能防范全部的威胁

防火墙安全策略的制定建立在已知的安全威胁上，所以防火墙能够防范已知的安全威

胁。但是,对于一些未知的安全威胁(如采用最新操作系统漏洞的网络攻击等)防火墙将无能为力。所以,在现在的网络安全实施方案中,在采取了防火墙技术的同时,还要综合采用入侵检测、入侵保护等技术,最好能够实现彼此之间的联动效果。

3. 防火墙不能防止感染了病毒的软件或文件的传输

随着技术的发展,虽然目前主流的防火墙可以对通过的所有数据包进行深度的安全检测,已决定是否允许其通过,但一般只会检查源 IP 地址、目的 IP 地址、TCP/UDP 端口及网络服务类型,较新的防火墙技术也可以通过应用层协议决定某些应用类型是否通过,但对于这些协议所封装的具体内容防火墙并不检查。所以,即使是最先进的数据包过滤技术在病毒防范上也是不适用的,因为病毒的种类太多,操作系统多种多样,而且目前的病毒编写技术很容易将病毒隐藏在数据中。

正因为以上原因,所以在进行单位网络的安全设计和部署时,除防火墙等安全技术和产品外,还需要使用防病毒系统。对于单位内部网络,建议使用企业级防病毒系统。

4. 防火墙不能防范内部用户的恶意破坏

据相关资料统计,目前局域网中有 80%以上的网络破坏行为是由内部用户所为,如在局域网中窃取其他主机上的数据、对其他主机进行网络攻击和散布计算机病毒等。这些行为都不通过位于局域网出口处的防火墙,防火墙对其无能为力。

5. 防火墙本身也存在安全问题

防火墙的工作过程要依赖于防火墙操作系统,与平常所使用的 Windows、Linux 等操作系统一样,防火墙操作系统也存在安全漏洞,而且防火墙的功能越强、越复杂,其漏洞就会越多。目前,在 IP 网络中使用的防火墙是基于 TCP/IP 模型实现的,而 TCP/IP 本身就存在安全问题(详细内容见本书第 5 章)。所以,影响 TCP/IP 安全的因素同样会影响防火墙的安全,防火墙在功能设计上就存在安全隐患。例如,如果防火墙要允许用户使用 HTTP 服务就必须开放 TCP 80 端口,允许用户使用 FTP 服务至少要开放 TCP 20 端口,但防火墙却无法防范针对已开放端口的 DoS、DDoS 等攻击等。所以,防火墙在高安全性方面的缺陷驱使用户追求更高安全性的解决方案。

6. 人为因素在很大程度上影响了防火墙的功能

防火墙仅仅提供了安全策略,但具体策略的配置和应用都需要由网络管理员来完成,即使是最智能化的防火墙也不可能会了解用户的安全需求,也不会自动识别所有的安全威胁。网络管理员的知识水平、网络管理员对单位网络安全需求的正确定位及网络管理员对具体使用的防火墙产品的熟悉程度等人为因素,在很大程度上决定了防火墙的实际应用效果。

8.3 防火墙的基本类型

作为内部网络与外部公共网络之间的一道屏障,防火墙是最先受到人们重视的网络安全产品之一。对于防火墙的工作类型,可以根据不同的方式进行分类。例如,按照防火墙对数据包处理方式的不同,可以分为包过滤防火墙和代理防火墙(也称“应用层网关防火墙”)两大体系,前者主要有以色列的 Chechpoint 防火墙和 Cisco PIX 防火墙,后者主要有 AI 公司的 Cauntlet 防火墙。考虑到读者的需要,本节则从防火墙的体系结构(或架构)入手,介绍防火墙的基本类型。

8.3.1 包过滤防火墙

包过滤防火墙是最早使用的一种防火墙技术，它在网络的进出口处对通过的数据包进行检查，并根据已设置的安全策略决定数据包是否允许通过。

1. IP 分组的组成

要学习包过滤防火墙的功能，就需要掌握数据包（IP 分组）的组成结构和功能。IP 分组的结构如图 8-4 所示。

<table>
<tr><td>版本(4)</td><td colspan="2">头长度(4)</td><td colspan="2">服务类型(8)</td><td colspan="2">部长度(16)</td></tr>
<tr><td colspan="5">标识(16)</td><td>标志(3)</td><td>段位移(13)</td></tr>
<tr><td colspan="2">生存期(8)</td><td colspan="3">协议(8)</td><td colspan="2">头校验和(16)</td></tr>
<tr><td colspan="7">源 IP 地址(32)</td></tr>
<tr><td colspan="7">目的 IP 地址(32)</td></tr>
<tr><td colspan="7">IP 选项(如果有，0 或 32)</td></tr>
<tr><td colspan="7">数据</td></tr>
</table>

图 8-4 IP 头格式

图中，除“数据”之外的部分称为“IP 头部”。IP 头部共占有 20 个字节，表 8-1 对 IP 头部的各个组成域进行了简单的描述。

表 8-1 IP 头部的功能描述

名　　称	描　　述
版本(VERS)	表明了一个数据包采用的是因特网协议的哪个版本。对于 IPv4，这个域的值为 4
头长度(HLEN)	以字节为单位的报头长度
服务类型(Type of Service)	数据包的处理方式，前三位是优先级
总长度(Total Length)	报头和数据的总长度
标识(Indentification)	唯一的 IP 数据包值，可以理解为 IP 报文的序列号，用于识别潜在的重复报文等
标志(Flags)	指出数据包是否存在
段位移(Frag Offset)	也称为片偏移，它是指对数据包分片以允许因特网上的不同 MTU
生存期(Time to Live，TTL)	报头的存活时间，一旦该计数值减为 0，该报就被丢弃。TTL 用于限制一个 IP 包所经历的站点数。正常设为 64，最大设为 255，TTL 每经过一个路由器便减 1。当值为 0 时，数据包被丢弃。同时，路由器向发送者返回一个 ICMP 超时信息。通常数据包只会由于网络存在路由回路而被丢弃。例如，当第一台路由器认为到达某一目的端的路径要经过第二台路由器，而第二台路由器又认为该路径应经过第一台路由器，这时会发生什么情况呢？当第一台路由器接收到一个发往该目的地址的数据包时，它会将数据包转发给第二台路由器，而第二台路由器又会将数据包重新转发给第一台路由器，然后第一台路由器又将包转发回第二台路由器。如果没有 TTL，这个包就会在这两台路由器构成的回路中永远转下去。这样的回路在大的网络中经常会出现
协议(Protocol)	发送数据包的上层(第四层)协议

名　称	描　述
头校验和(Header Checksum)	报头上的完整性检查。头校验用来确认接收到的 IP 报头中有没有差错。头校验和只由 IP 报头中的各个域计算得来,而与 IP 包的净荷无关,IP 包净荷的校验则是高层协议的工作。如果目的地计算的校验和与报文所含的校验和不同,那么这个数据包就会被丢弃
源 IP 地址(Source IP address)	标识发送方通信终端设备的 IP 地址
目的 IP 地址(Destination IP address)	标识下一站通信终端设备的 IP 地址
IP 选项(IP Options)	网络测试、调试和安全等功能选项
数据(Data)	需要被传输的数据

2. 包过滤防火墙的工作原理

包过滤(packet filter)是在网络层中根据事先设置的安全访问策略(过滤规则),检查每一个数据包的源 IP 地址、目的 IP 地址及 IP 分组头部的其他各种标志信息(如协议、服务类型等),确定是否允许该数据包通过防火墙。其实,从早期的包过滤防火墙开始,防火墙除能够根据 IP 分组的头部信息进行数据包的检查外,还能够检查 TCP 和 UDP 协议及使用的端口,并将其作为数据包的过滤规则。为此,包过滤防火墙同时工作在 OSI 参考模型的网络层和传输层。

包过滤防火墙中的安全访问策略(过滤规则)是网络管理员事先设置好的,主要通过对进入防火墙的数据包的源 IP 地址、目的 IP 地址、协议及端口进行设置,决定是否允许数据包通过防火墙。

例如,如果拒绝从 IP 地址为 172.16.1.100 的主机发出的数据包通过防火墙,则可以通过类似于下面的一条命令来实现:

```
deny ip host 172.16.1.100 any
```

如果允许使用 80 号端口的 TCP 协议和使用 20 号端口的 UDP 协议的数据包通过,则可以通过类似于下面的两条命令来实现:

```
permit tcp any any eq 80
permit udp any any eq 20
```

网络管理员可以根据网络安全的实际需要,通过相应的命令行允许(permit)或拒绝(deny)数据包通过。

如图 8-5 所示,当网络管理员在防火墙上设置了过滤规则后,在防火墙中会形成一个过滤规则表。当数据包进入防火墙时,防火墙会将 IP 分组的头部信息与过滤规则表进行逐条比对,根据比对结果决定是否允许数据包通过。假设某一防火墙的过滤规则表中只有以下的 4 条规则(实际应用中要远远超过 4 条):

```
deny ip host 172.16.1.100 any
permit tcp any any eq 80
permit udp any any eq 20
deny ip any any
```

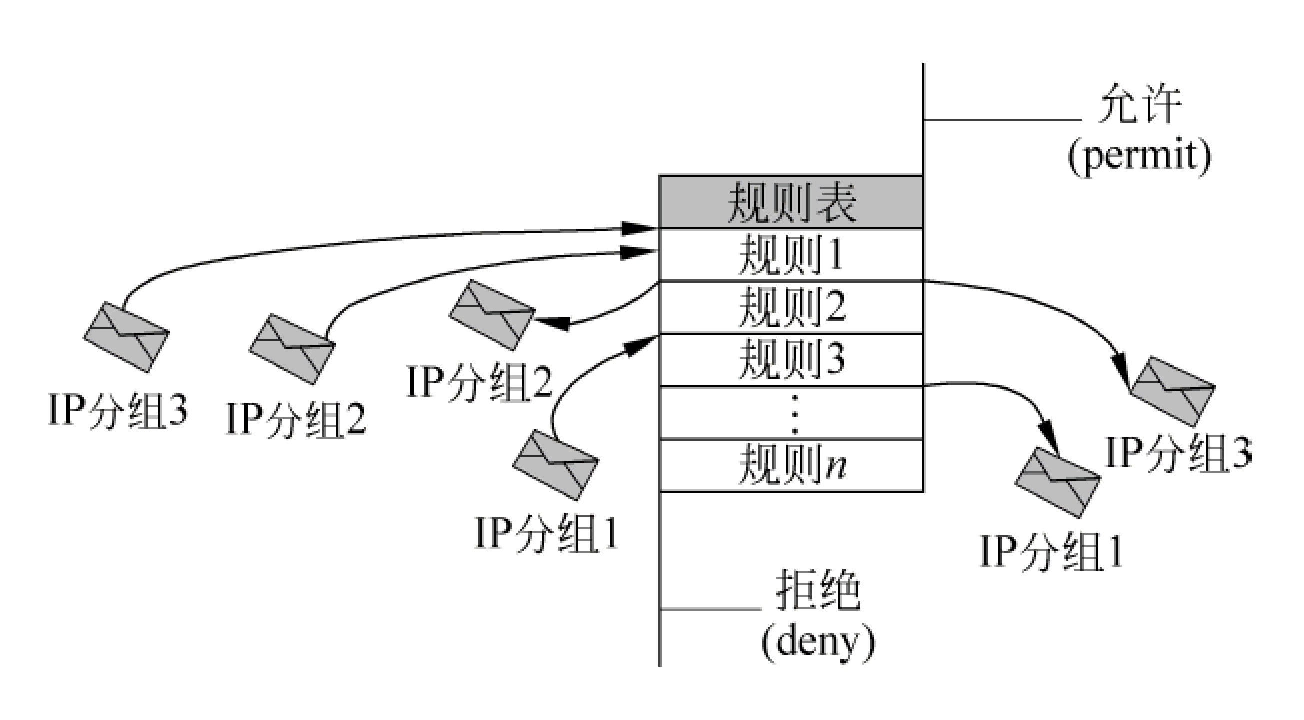


图 8-5　包过滤防火墙工作示意图

防火墙的过滤规则表其实是一个访问控制列表(Access Control List,ACL),当数据包进入防火墙时,防火墙首先提取 IP 分组的头部信息,然后再与 ACL 中的条目从上到下进行一一比对。如果第一条规则不匹配,就开始检查第二条规则,依此类推。当 ACL 中的某一条规则匹配时,防火墙开始执行该规则,不再进行以下条目的检查。

3. 包过滤防火墙的应用特点

包过滤防火墙是一种技术非常成熟、应用非常广泛的防火墙技术,具有以下主要特点。

(1) 过滤规则表需要事先进行人工设置,规则表中的条目根据用户的安全要求来定。

(2) 防火墙在进行检查时,首先从过滤规则表中的第一个条目开始逐条进行,所以过滤规则表中条目的先后顺序非常重要。当网络管理员要添加新的过滤规则时,不能简单地添加在规则表的最前面或最后面,而是要视具体规则的应用特点来确定其位置。

(3) 由于包过滤防火墙工作在 OSI 参考模型的网络层和传输层,所以包过滤防火墙对通过的数据包的速度影响不大,实现成本较低。但包过滤防火墙无法识别基于应用层的恶意入侵,例如恶意 Java 小程序、携带在电子邮件中的病毒等。另外,包过滤防火墙不能识别 IP 地址的欺骗,内部非授权的用户可以通过伪装成为合法 IP 地址的使用者来访问外部网络,同样外部被限制的主机也可以通过使用合法的 IP 地址来欺骗防火墙进入内部网络。

8.3.2 代理防火墙

代理防火墙也称为应用层网关防火墙。这里的代理(proxy)类似于今天社会上的中介公司或经纪人,即真正参与交流的双方必须借助于第三方(即代理)来完成,否则他们之间是完全隔离的。

1. 代理防火墙的工作原理

代理防火墙具有传统的代理服务器和防火墙的双重功能。如图 8-6 所示,代理服务器位于客户机与服务器之间,完全阻挡了二者间的数据交流。从客户机来看,代理服务器相当于一台真正的服务器;而从服务器来看,代理服务器仅是一台客户机。代理防火墙的工作原理是将每一个从内部网络到外部网络的连接请求,分为两个组成部分:首先,代理服务器根据安全过滤规则决定是否允许这个连接,如果允许则代理服务器就代替客户机向外部网络中的服务器发出请求;然后,当代理服务器接收到外部网络中的服务器发送回来的响应数据包时,同样要根据安全过滤规则决定是否让该数据包进入内部网络,如果允许这个数据包进入,代理服务器便将其转发给内部网络中发起请求的客户机。

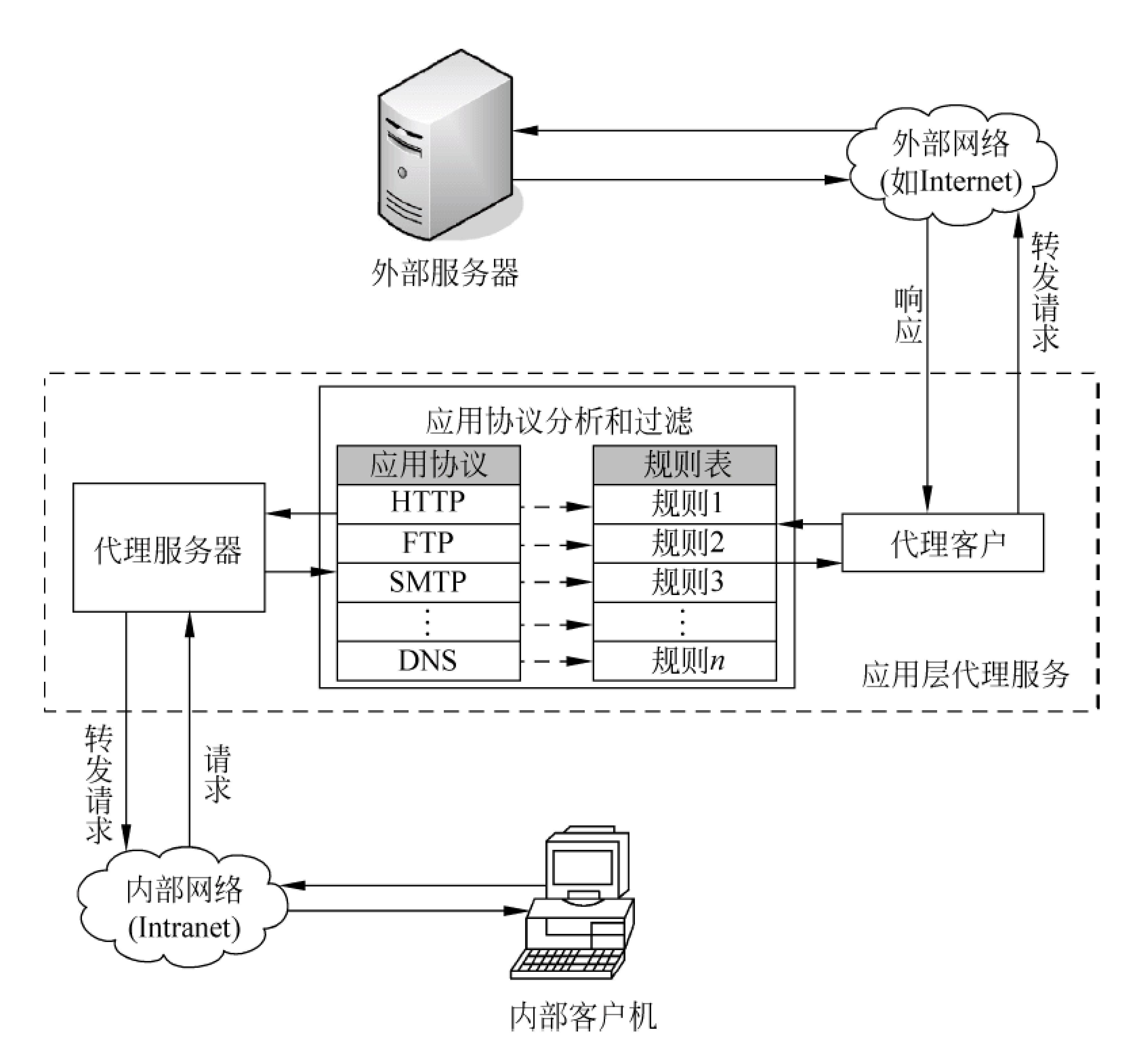


图 8-6　代理防火墙的工作示意图

由图 8-6 可以看出，代理防火墙无论是接收到内部网络发出的请求，还是接收外部服务器返回的响应，都要进行安全策略（协议分析和规则过滤）的处理。只有与安全策略相匹配的数据才能交给代理服务器继续进行处理。例如，当内部网络中的客户机向外部的某一台 Web 服务器发出 http 访问请求时，代理服务器首先根据安全策略检查是否允许 http 请求通过。如果代理服务器允许该 http 请求通过，则将其交给代理服务器进行处理。从外部的 Web 服务器返回的响应数据也要经过相同的处理过程。

在整个通信过程中，网络的连接和转发对用户来说是完全透明的，所有操作都由代理防火墙自动处理。目前，代理防火墙可以支持对常见的 HTTP、HTTPS、SSL、SMTP、POP3、IMAP、SNMP、Telnet 和 FTP 等应用层协议的代理，同时一些新的应用层协议还会逐渐加入其中。

2. 代理防火墙的应用特点

包过滤防火墙可以根据 IP 分组的头部信息来决定数据包是否允许通过，但它无法根据应用层的协议进行访问控制，所以包过滤防火墙主要应用于安全功能较为单一的中小型网络。对于大中型企业网络来说，代理防火墙可以通过对应用层协议的控制，实现对具体应用的控制和安全管理。代理防火墙具有以下的主要特点。

(1) 代理防火墙可以针对应用层进行检测和扫描，可有效地防止应用层的恶意入侵和病毒。

(2) 代理防火墙具有较高的安全性。由于每一个内外网络之间的连接都要通过代理服务器的介入和转换，而且在代理防火墙上会针对每一种网络应用（如 HTTP）使用特定的应用程序来处理。当一个数据包到达代理防火墙时，代理防火墙首先检查是否有针对该数据

包的应用层协议，如果没有则直接丢弃。

(3) 代理服务器通常拥有高速缓存，缓存中保存了用户最近访问过的站点内容。当下一个用户要访问同样的站点时，代理服务器就直接利用缓存中的内容，而不需要再次建立与远程服务器之间的连接，节约了时间和网络资源，在一定程度上提高了内部用户访问外部服务器的速度。

(4) 代理防火墙的缺点是对系统的整体性能有较大的影响，系统的处理效率会有所下降，因为代理型防火墙对数据包进行内部结构的分析和处理，这会导致数据包的吞吐能力降低(低于包过滤防火墙)。

8.3.3 状态检测防火墙

状态检测防火墙又称动态包过滤防火墙，是在传统包过滤防火墙的基础上发展起来的。因此，将传统的包过滤防火墙称为静态包过滤防火墙，而将状态检测防火墙称为动态包过滤防火墙。

1. 静态包过滤的缺陷

要掌握状态检测防火墙的工作原理，其实是掌握静态包过滤和动态包过滤技术的区别。静态包过滤防火墙根据预先定义好的过滤规则检查每一个数据包，从而决定该数据包是否通过防火墙。过滤规则基于数据包的头部信息进行制定，其中包括源 IP 地址、目的 IP 地址、传输协议(如 TCP、UDP 和 ICMP 等)、TCP/UDP 端口和 ICMP 消息等类型。静态包过滤防火墙要遵循的一条基本准则是“最小特权原则”，即明确允许某些数据包的通过，而拒绝其他的一切数据包。

由于静态包过滤技术要检查进入防火墙的每一个数据包，所以在一定程度上影响了网络的通信速度。另外，静态包过滤技术固定地根据包的头部信息进行规则的匹配，这种方法在遇到利用动态端口的应用协议时就会出现问题。例如，FTP 通信在整个通信过程中使用了两种类型的 TCP 连接：控制连接和数据连接。其中，控制连接用于客户端与服务器之间交互协商与命令的传输，而数据连接用于客户端与服务器之间传输数据。首先来看控制连接的建立过程：客户端向服务器固定的 21 号端口发起 TCP 连接请求希望建立 FTP 控制连接。对于静态包过滤防火墙来说，如果不允许用户使用 FTP 服务，就可以直接在防火墙上关闭 TCP 21 端口。但是，如果静态防火墙允许用户使用 FTP 服务时情况又是怎么样呢？这时当客户端向服务器的 21 号端口发起 TCP 连接请求时，如果服务器同意与客户端建立连接，首先客户端与服务器会在控制连接信息中交换用于数据传输的 TCP 端口，这一端口一般在 1024～65535 之间。然后客户端与服务器之间使用彼此交换后的 TCP 端口进行数据传输，即进入数据连接过程。由以上过程可以看出，数据连接中使用的端口是动态的，即每次使用的端口都有可能不同，而静态防火墙无法知道哪些端口需要打开。如果要在静态防火墙上允许用户使用 FTP 服务，就需要将所有可能的端口打开，同时在通信结束后防火墙也不会自动关闭这些端口。这也会存在一定的安全隐患。

2. 状态检测技术及优势

在静态包过滤技术中检查的数据包称为无状态包。无状态包之间是独立存在的，防火墙关心的仅是数据包的静态信息(如源 IP 地址、目的 IP 地址和端口等)，而不关心数据包的历史和未来情况。动态包过滤技术中检查的数据包称为有状态包。有状态包之间是关联

的，即多个数据包之间会存在一些共性。例如，在一次FTP通信过程中，所有的控制连接和数据连接之间都存在共性：由谁（以客户端的IP地址为主）发出请求、由谁（以服务器的IP地址为主）得到响应及在数据传输中使用的TCP端口是什么等。

状态检测技术即动态包过滤技术。状态检测防火墙检查的不仅仅是数据包中的头部信息，而且会跟踪数据包的状态，即不同数据包之间的共性。还以前面介绍的FTP通信过程为例，在状态检测防火墙中，一旦允许客户端与服务器之间的数据传输，状态检测防火墙就会在缓存中记录最近的连接信息：是某一特定IP地址的FTP应用程序与某一特定IP地址的服务器之间使用某一TCP端口建立的连接。当这一FTP通信过程中的后续数据包进入防火墙时，防火墙就会与缓存中的连接信息进行匹配，如果相同就被允许通信。

状态检测防火墙的关键技术是实现连接的跟踪功能。对于单一连接的协议（如SMTP、HTTP等）来说相对比较简单，只需要数据包的头部信息就可以进行跟踪。但是，对于一些复杂的协议（如FTP、一些多媒体通信协议及一些数据库通信中使用的协议等），除了使用一个公开的连接端口建立控制连接外，在通信过程中还会动态建立子连接进行数据传输，而子连接（一般为数据连接）中使用的端口是在主连接（控制连接）中通过协商得到的随机值。因此，对于这类复杂的协议，如果使用静态包过滤技术就只能打开所有可能使用到的端口，带来了安全隐患。对于状态检测防火墙，则能够进一步分析主连接中的信息，识别出所协商的子连接的端口，并在防火墙上将其打开，连接结束时自动关闭，保证了系统的安全性。

3. 状态检测防火墙的工作过程

状态检测防火墙的工作过程如图8-7所示。在状态检测防火墙中有一个状态检测表，它由规则表和连接状态表两部分组成。状态检测防火墙的工作过程是：首先利用规则表进行数据包的过滤，此过程与静态包过滤防火墙基本相同。如果某一个数据包（如"IP分组B1"）在进入防火墙时，规则表拒绝它通过，则防火墙直接丢弃该数据包，与该数据包相关的后续数据包（如"IP分组B2"、"IP分组B3"等）同样会被拒绝通过。

如果某一个数据包（如"IP分组A1"）在进入防火墙时，与该规则表中的某一条规则（如是"规则3"）相匹配，并允许其通过。此时，状态检测防火墙会分析已通过的数据包（"IP分组A1"）的相关信息，并在连接状态表中为这一次通信过程建立一个连接（如"连接1"）。之后，当同一通信过程中的后续数据包（如"IP分组A2"、"IP分组A3"、…、"IP分组An"）进入防火墙时，状态检测防火墙不再进行规则表的匹配，而是直接与连接状态表进行匹配。由于后续的数据包与已允许通过防火墙的数据包"IP分组A1"具有相同的连接信息，所以会直接允许其通过。

4. 跟踪连接状态的方式

状态检测防火墙跟踪连接状态的方式取决于所使用的传输层协议，下面进行简要的分析和介绍。

（1）TCP数据包。当建立一个TCP连接时需要进行三次握手（详见本书第5章），其中发起连接请求的数据包中包含有SYN的标志。除特殊设置外，状态检测防火墙可以让由内部发起的TCP连接请求通过，同时在缓存中记录这次连接的相关信息，而丢弃所有外部网络中发起的TCP连接请求。如果从外部网络中传入状态检测防火墙的数据包是响应数据包，则允许其进入，然后再与相关策略进行匹配，决定是否允许进入内部网络。

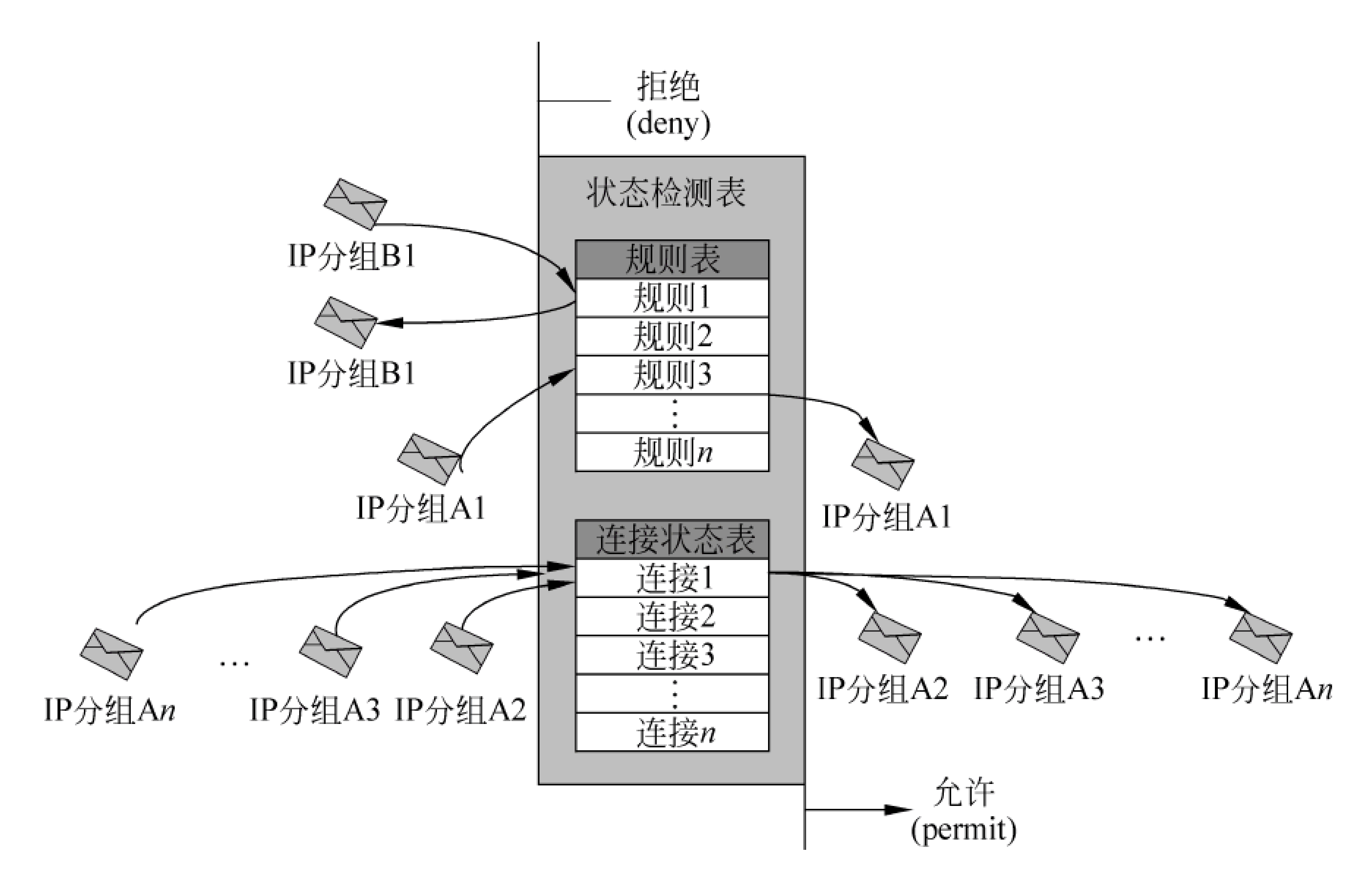


图 8-7 状态检测防火墙的工作示意图

以上特殊设置主要是在防火墙上通过 NAT 功能建立的内部私有 IP 地址与外部公有 IP 地址之间的一对一连接，即为了使外部网络中的用户能够访问内部网络中的服务器而设置的内外 IP 地址之间的静态映射。

（2）UDP 数据包。与 TCP 数据包相比，UDP 数据包相对要简单得多，位于传输层的一个 UDP 数据包除数据外，只包含源端口、目的端口、报文长度和校验和 4 个区域的头部信息，如图 8-8 所示。

源端口（2 字节）	目的端口（2 字节）
报文长度（2 字节）	校验和（2 字节）
数据	

图 8-8 UDP 数据包的结构

同时，UDP 数据包的传输不需要进行三握手过程。这使得状态检测防火墙不能采用对 TCP 数据包的跟踪方式来跟踪 UDP 数据包。但是，通过跟踪数据包的状态情况就可以解决这一问题。因为不管是 TCP 连接还是 UDP 连接，都需要由用户发出连接请求，所以当内部网络中的客户端向外部网络中的服务器发出连接请求时，如果状态检测防火墙允许这一请求通过，就会在缓存中保存相应的连接信息。这样，对从外部网络中进入防火墙的 UDP 数据包，就可以在检查它的地址和协议后，通过与缓存中保存的连接信息进行比较，决定是否允许该 UDP 数据包进入内部网络。

因以上分析可知，对于状态检查防火墙来说，除特殊设置外，所有从外部网络发起的连接请求是不允许通过的。

5. 状态检测防火墙的应用特点

状态检测防火墙综合应用了静态包过滤防火墙的成熟技术，并对其功能进行了扩展，可在 OSI 参考模型的多个层次对数据包进行跟踪检查，其实用性得到了加强。状态检测防火墙具有以下主要特点。

（1）与静态包过滤防火墙相比，采用动态包过滤技术的状态检测防火墙通过对数据包的跟踪检测技术，解决了静态包过滤防火墙中某些应用需要使用动态端口时存在的安全隐患，解决了静态包过滤防火墙存在的一些缺陷。

(2) 与代理防火墙相比,状态检测防火墙不需要中断直接参与通信的两台主机之间的连接,对网络速度的影响较小。

(3) 状态检测防火墙具有新型的分布式防火墙的特征。状态检测防火墙产品还可以使用分布式探测器,这些探测器安置在各种应用服务器和其他网络设备上。所以,状态检测防火墙不但可以对外部网络的攻击进行检测,同时可以对内部网络的恶意破坏进行防范。这使状态检测防火墙已超出了对防火墙的传统定义。

(4) 状态检测防火墙的不足主要表现为:对防火墙 CPU、内存等硬件要求较高,安全性主要依赖于防火墙操作系统的安全性,安全性不如代理防火墙。其实,状态检测防火墙提供了比代理防火墙更强的网络吞吐能力和比静态包过滤防火墙更高的安全性,在网络的安全性和数据处理效率这两个相互矛盾的因素之间进行了较好的平衡。

8.3.4 分布式防火墙

分布式防火墙是近年来发展起来的一种新型的防火墙体系结构,它将传统的防火墙技术和分布式网络应用进行了有机结合,具有广泛的研究和应用前景。

1. 传统防火墙的不足

虽然本章前面介绍的几类传统防火墙仍然是现代计算机网络安全防范的支柱,但在安全要求较高的大型网络中存在一些不足,主要表现如下。

(1) 结构性限制。传统的防火墙属于一种边界安全设备,所以也称为边界防火墙。但边界防火墙的工作机理依赖于网络的物理拓扑结构。如今,越来越多的跨地区企业利用 Internet 来构架自己的网络,致使企业内部网络已基本上成为一个逻辑概念,所以用传统的方式来区别内外网络已非常困难。

(2) 防外不防内。虽然有些传统的防火墙(如状态检测防火墙)可以防止内部用户的恶意破坏,但在绝大多数情况下,用户使用和配置防火墙时还是主要防止来自外部网络的入侵。

(3) 效率问题。传统防火墙把检查机制集中在网络边界处的单一节点上,所以防火墙容易形成网络的瓶颈。虽然防火墙产品可以通过提高处理能力来尽可能地解决瓶颈问题,但网络应用的复杂性却在另一方面增加了防火墙的压力。

(4) 故障问题。传统防火墙本身也存在着单点故障问题。一旦处于安全节点上的防火墙出现故障或被入侵,整个内部网络将完全暴露在外部攻击者的面前。

2. 分布式防火墙的概念

为了解决传统防火墙正在面临的问题,美国 AT&T 实验室研究员 Steven M. Bellovin 于 1999 年在他的论文"分布式防火墙(Distributed Firewalls,DFW)"中首次提出了分布式防火墙的概念。在该论文中提供了 DFW 的方案:策略集中定制,在各台主机上执行,日志集中收集处理。根据 DFW 所需要完成的功能,分布式防火墙系统由以下三部分组成:

(1) 网络防火墙。承担着与传统边界防火墙相同的职能,负责内外网络之间不同安全域的划分。同时,用于对内部网各子网之间的防护。与传统边界防火墙相比,分布式防火墙中的网络防火墙增加了一种用于对内部子网之间的安全防护,这样使分布式防火墙实现了对内部网络的安全管理功能。

(2) 主机防火墙。为了扩大防火墙的应用范围,在分布式防火墙系统中设置了主机防火墙。主机防火墙驻留在主机中,并根据相应的安全策略对网络中的服务器及客户端计算

机进行安全保护。

根据实现方式的不同，主机防火墙可以分为主机驻留和嵌入操作系统内核两种方式。其中，主机驻留是指防火墙功能驻留在主机的内存中，对主机进行实时的安全保护。主机驻留类似于单机中使用的个人防火墙，它只负责对本地主机进行安全保护，不信赖除本地主机外的其他主机。嵌入操作系统内核方式主要防范由于操作系统自身存在的安全漏洞而引起的安全问题，如 Windows XP/2003/Vista 自带的“Windows 防火墙”。这种类型的主机防火墙的安全程序直接嵌入到操作系统的内核中运行，直接接管网卡，检查进入操作系统的所有数据包。

（3）中心管理服务器。是整个分布式防火墙的管理核心，负责安全策略的制定、分发及日志收集和分析等操作。

3. 分布式防火墙的工作模式

分布式防火墙的基本工作模式是：由中心管理服务器统一制定安全策略，然后将这些定义好的策略分发到各个相关节点。而安全策略的执行则由相关主机节点独立实施，由各主机产生的安全日志集中保存在中心管理服务器上。分布式防火墙的工作模式如图 8-9 所示。

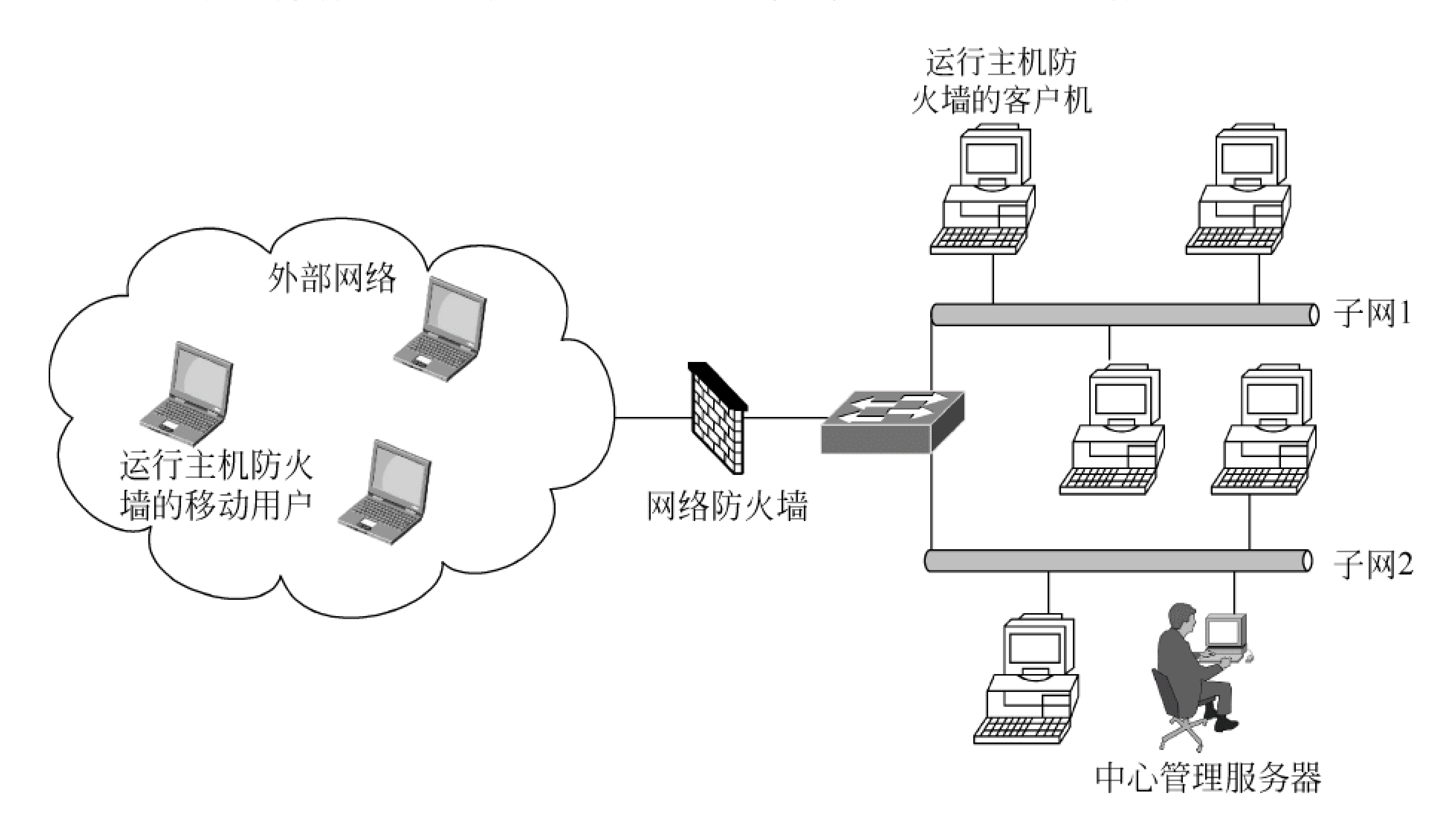


图 8-9　分布式防火墙的工作模式

由图 8-9 可以看出，在分布式防火墙中已不再完全依赖网络的拓扑结构来定义不同的安全域，可信赖的内部网络发生了概念上的变化，内部网络已成为一个逻辑上的网络，从而打破了传统防火墙对网络拓扑的依赖。但是，各主机节点在处理数据包时，必须根据中心管理服务器所分发的安全策略来决定是否允许某一数据包通过防火墙。

4. 分布式防火墙的应用特点

由于在分布式防火墙中采用了中心管理服务器对整个防火墙系统进行集中管理的方式，其中安全策略在统一制定后被强行分发到各个节点，所以分布式防火墙不仅保留了传统防火墙的优点，同时还解决了传统防火墙在应用中存在的对网络物理拓扑结构的依赖、内部恶意破坏和网络应用瓶颈等不足。分布式防火墙的应用优势主要表现在如下方面。

（1）增加了针对主机的入侵检测和防护功能，加强了对来自内部网络的攻击防范，可以实施全方位的安全策略。

（2）提高了系统性能，克服了结构性瓶颈问题。

(3) 与网络的物理拓扑结构无关,支持 VPN 和移动计算等应用,应用更加广泛。

5. 分布式防火墙产品

虽然分布式防火墙技术的提出相对较晚,但相应的产品非常丰富。目前,从总体来看,国外的一些著名网络设备制造商(如 3COM、Cisco 和美国网络安全系统公司等)在分布式防火墙技术方面更加先进,所提供的产品性能也比较高。在众多的分布式防火墙产品中,一般采用"软件+硬件"和"纯软件"两种形式。采用"软件+硬件"的分布式防火墙,一般网络防火墙使用硬件形式,而主机防火机采用软件形式。

例如,3COM 公司近期发布的嵌入式防火墙就是一种基于"硬件+软件"的分布式防火墙产品。其中,主机防火墙被嵌入到网卡中,通过中心管理服务器来实现集中管理。这种嵌入式防火墙技术把硬件解决方案的强健性和集中式管理软件解决方案的灵活性结合在一起,从而创建了一种更加全面的安全基础架构。

再如,北京安软科技有限公司推出的一个具备三层过滤结构的软件防火墙产品 EverLink DFW。它依靠包过滤、木马过滤和脚本过滤的三层过滤检查,保护个人计算机在正常使用网络时不会受到恶意的攻击,提高了网络的安全性。同时,为方便管理,所有分布在各主机节点的主机防火墙的安全策略由中心管理服务器进行统一设置和维护,降低了分布式防火墙的使用成本,同时提高了安全保障能力。

8.4 个人防火墙技术

本章前面介绍的防火墙概念和主要实现技术一般都是针对单位用户而言的,所以将这类防火墙也称为企业级防火墙。企业级防火墙虽然功能强大,但价格昂贵、配置困难、维护复杂,需要具有一定安全知识的专业人员来配置和管理。近年来,随着以家庭用户为代表的个人计算机的不断普及,个人防火墙技术开始出现并得到了广泛应用。

8.4.1 个人防火墙概述

与企业级防火墙相比,个人防火墙的出现相对较晚,但应用功能较为全面,而且策略的设置比较简单,适合普通用户的应用需求。

1. 个人防火墙的产生动因

随着以 Internet 为主的互联网技术在商业领域中应用价值的不断提升,为了提高企业的竞争力并追求企业效益的高大化,现在大大小小的企业都接入到了互联网。所有接入到互联网的企业都存在内部机密数据被窃取、修改或盗用的危险,为解决这一安全问题,企业级防火墙得到了用户的普遍重视和应用。

从 1985 年第一个在 Cisco 网络产品的操作系统(IOS)上提供的防火墙到现在,防火墙产品已经从最初的静态包过滤技术发展到随后的代理、动态包过滤(状态检测)及现在的分布式防火墙技术。由于企业网络应用的多样性和复杂性,虽然企业级防火墙从技术上不断推陈出新,以应对不断出现的网络安全威胁,但企业级防火墙价格昂贵、配置和管理复杂、缺乏结构的灵活性、防范策略总滞后于安全威胁,在很大程度上影响了企业级防火墙产品向家庭、小型办公用户的扩展。为保护单机用户接入互联网时的安全,防止个人计算机上信用卡、银行账号等私有信息的泄露和窃取,防止计算机病毒及各种恶意程序对个人计算机的入

侵和破坏,个人防火墙产品应运而生。

2. 个人防火墙的概念

个人防火墙是一套安装在个人计算机上的软件系统,它能够监视计算机的通信状况,一旦发现有对计算机产生危险的通信就会报警通知管理员或立即中断网络连接,以此实现对个人计算机上重要数据的安全保护。

个人防火墙是在企业防火墙的基础上发展起来的,个人防火墙采用的技术也与企业防火墙基本相同,但在规则的设置、防火墙的管理等方面进行了简化,使非专业的普通用户能够容易地安装和使用。

Windows 操作系统是目前应用最为广泛的个人计算机操作系统。为了实现对 Windows 操作系统的安全保护,Windows 本身提供了防火墙功能。目前市面上推出了大量基于 Windows 操作系统的个人防火墙产品。其中,国外知名品牌主要有 Norton、PC Cilin 等,国内品牌主要有天网个人版防火墙、瑞星个人防火墙和金山毒霸网络个人防火墙等。同时,目前正在兴起的 Linux 操作系统本身就内置了强大的个人防火墙功能。

8.4.2 个人防火墙的主要功能

对于连接到因特网上的个人计算机,存在的最大安全隐患是个人的私有信息被窃取或被破坏,以及个人计算机被攻击者用作盗取他人关键信息的跳板。同时,还存在恶意软件造成的网络或系统资源的浪费。为了防止安全威胁对个人计算机产生的破坏,个人防火墙产品应提供以下的主要功能。

1. 防止 Internet 上用户的攻击

个人防火墙可以保护连接到 Internet 上的主机不被攻击,尤其是长期接入到 Internet 上的个人计算机。目前,长期接入到 Internet 上的个人计算机越来越多,这些计算机不仅仅是作为浏览 Web 网页及下载文件使用,同时还可以作为 Web、FTP 等服务器为 Internet 上的用户提供服务。随着动态 DNS 技术的广泛应用,一般一台能够与 Internet 连接的个人计算机就可以成为一台 Web、FTP 和电子邮件等服务器。个人防火墙可以在很大程度上保护这些个人服务器系统。

2. 阻断木马及其他恶意软件的攻击

计算机木马可以通过网页浏览、电子邮件和软件下载等诸多方式进入个人计算机,在计算机上开设一个后门。然后攻击者通过这个后门进入计算机,破坏、窃取用户的个人信息。个人防火墙可以阻断来自外部主机的木马入侵。

现在较新的个人防火墙还针对个人计算机用户存在的安全风险,提供了反钓鱼、反流氓软件、防 ARP 欺骗和 DHCP 欺骗等功能,最大限度地保护了个人计算机的安全。

3. 为移动计算机提供安全保护

随着家庭办公等移动办公方式的兴起,单位员工可以在自己家里或外出时利用 VPN 方式连接到单位内部的网络,实现与单位内部计算机用户相同的资源访问功能。如果移动计算机没有个人防火墙的保护,当其以 VPN 方式接入到单位内部网络时,单位内部的网络将暴露在 Internet 上,攻击者将把这台 VPN 终端作为进入单位内部网络的桥梁。

4. 与其他安全产品进行集成

个人防火墙除能够满足个人用户的一些需求外,还可以与其他的网络安全产品进行集

成，在安全防范上产生联动效应，最大范围地提供安全性。目前主流的方法是将个人防火墙与防病毒软件进行集成，将两者的功能结合起来。例如，Norton、瑞星和金山等防病毒软件一般都集成了个人防火墙功能。

随着技术的发展，个人防火墙的功能也在不断发展和完善，例如自动检测个人计算机操作系统存在的安全漏洞、为操作系统提供补丁安装服务、提供为个人计算机上资源的授权访问及提供入侵检测功能等。

8.4.3 个人防火墙的主要技术

由于个人防火墙是在企业级防火墙的基础上发展起来的，所以个人防火墙所采用的技术主要与企业级防火墙基本相同，但也存在一些应用特点。下面介绍个人防火墙所使用的主要技术。

1. 基于应用层网关

典型的个人防火墙属于应用层网关类型，应用层网关也称为代理。应用层网关随时检测用户应用程序的执行情况，可以根据需要对特定的应用拒绝或允许。例如，当用户需要执行一个 FTP 应用程序时，可以允许文件的上传和下载，其他的应用可以被关闭。基于应用层的网关防火墙在企业防火墙的配置中比较复杂，但在个人防火墙的策略配置中却比较简单，用户需要什么服务就允许什么服务通过防火墙，该服务使用结束后可以及时关闭。

2. 基于 IP 地址和 TCP/UDP 端口的安全规则

如果要在个人防火墙上实现基于 IP 地址和 TCP/UDP 端口的控制将非常容易。例如，如果不允许某一台个人计算机使用 FTP 服务，就可以在个人防火墙上直接关闭 TCP 20 端口，这样即使有人想通过这台计算机利用 FTP 下载文件，其 FTP 的连接请求在个人防火墙上将被直接拒绝，根本无法建立与 FTP 服务器之间的控制连接。如果不允许访问某一站点，则可以直接在个人防火墙上拒绝将数据包发往该网站对应的 IP 地址。基于 IP 地址和 TCP/UDP 端口的安全规则其实就是一种静态包过滤技术。同样，静态包过滤防火墙存在的不安全因素在个人防火墙上也同样存在。

3. 端口“隐蔽”功能

下面看一个针对网络端口的扫描实例：假设通过端口扫描软件来对一台远程计算机进行端口扫描操作，如果远程计算机上的某一端口是开放的，扫描软件自然会收到该端口已打开的响应报文；如果该端口是关闭的，远程主机会返回一个拒绝连接的响应报文。从这一实例可以看出，不管端口是否关闭，扫描软件都会知道远程主机的存在。既然知道了远程主机的存在，就可以采取其他方式对其进行攻击。

而端口“隐蔽”会将主机上的端口完全隐藏起来，而不返回任何响应或拒绝响应的报文。由于不发送响应报文，所以它是一个非标准的连接行为。在个人防火墙上启用了端口“隐蔽”功能，则会隐蔽掉该计算机的存在。

4. 邮件过滤功能

一个标准的电子邮件通常具有几个重要特征：收发人邮箱名、收发人邮箱服务器的 IP 地址或域名、主题及信件内容（包括正文、关键字和附件）等相关字段，这些特征是邮件过滤技术判断、分析、统计和提取的依据。个人防火墙的邮件过滤功能可以对接收到的电子邮件的主要特征进行提取和分析，确定是否需要接收邮件或给用户相应的提示信息。

通过以上介绍,读者会发现个人防火墙虽然继承了企业级防火墙的技术和功能,但是个人防火墙的主要功能集中在防攻击、防木马及恶意软件的入侵、防病毒等方面,而不是对某一个网络的安全保护。

8.4.4 个人防火墙的现状及发展

个人防火墙为接入到 Internet 的个人计算机提供了所需要的安全保护,主要包括如下方面。

(1) 可有效地防范各种网络攻击。

(2) 高效的入侵检测、报警和日志收集与分析。

(3) 防火墙本身应该具有良好的容错性。

(4) 及时阻止攻击的继续,同时还应能对攻击源进行定位,并具有自我学习、扩充和更新规则的功能。

(5) 操作界面友好,操作过程简单、易学、易用,并具有在线安全策略的维护功能。

个人防火墙从产生到现在,已经经历了多次技术上的更新,从简单、单一的数据包拦截,到对应用层协议的分析,再到与防病毒、防入侵等安全功能的有机结合。在个人保密要求提高、网络开放性逐渐增大、攻击手段日益多样化的情况下,个人防火墙技术也紧随用户的安全需求发生着变化。与企业级防火墙相比,个人防火墙更多考虑的是实用性和灵活性,在实现方式上没有企业级防火墙那样复杂,在功能上没有企业级防火墙那样完备。由于个人防火墙是面向个人用户的,从结构上来讲只是一个端系统,并没有复杂的网络拓扑,从实现形式来讲也几乎都是一种纯软件的方式。

有关个人防火墙未来的发展,除技术的不断创新和功能的不断完善外,在实现形式上还需要从以下几个方面取得发展。

(1) 与网络设备集成。可将个人防火墙功能集成到 Modem、xDSL、Cable Modem 和无线 AP 等设备中,使个人防火墙成为这些网络设备的组成模块。

(2) 与防病毒软件集成,并实现与防病毒软件之间的安全联动。例如,同一网络安全厂商开发的防病毒软件和个人防火墙软件可以合并成同一个产品,而不是将个人防火墙作为防病毒软件的一个可选组件来存在。

(3) 使个人防火墙成为企业级防火墙的一个子系统,通过企业级防火墙对个人防火墙进行分布式管理。这一思想其实就是将个人防火墙作为分布式防火墙中的主机防火墙来存在。

8.5 实验操作 1 瑞星个人防火墙应用实例

个人防火墙主要是为解决网络上各类攻击问题而研制的个人信息安全产品,具有较为完备的规则设置功能,能有效地监控网络连接,保护网络不受攻击。本实验以 2008 版瑞星个人防火墙为例,通过对个人防火墙主要功能及配置方法的介绍,使读者对个人防火墙技术及使用有所了解。

8.5.1 瑞星个人防火墙的主要功能

下面是 2008 版瑞星个人防火墙的主要特性。

(1) 防火墙多账户管理。防火墙提供"管理员"和"普通用户"两种账户。防火墙提供的

切换账户功能可以在两种账户之间进行切换。管理员可以执行防火墙的所有功能，普通用户不能修改任何设置、规则，不能启动/停止防火墙，不能退出防火墙。且普通用户切换到管理员用户需要输入管理员用户的密码。

(2) 未知木马扫描技术。通过启发式查毒技术，当有程序进行网络活动的时候，对该进程调用未知木马扫描程序进行扫描，如果该进程为可疑的木马病毒，则提示用户。此技术提高了对可疑程序自动识别的能力。

(3) IE功能调用拦截。由于IE提供了公开的Com组件调用接口，有可能被恶意程序所调用。此功能是对需要调用IE接口的程序进行检查。如果检查为恶意程序，报警给用户。

(4) 反钓鱼和防木马病毒网站。提供了较为强大的、可以升级的黑名单规则库。库中管理了非法的、高风险、高危害的网站地址列表，符合该库的访问会被禁止。

(5) 模块检查。防火墙能够控制是否允许某个模块访问网络。当应用程序访问网络的时候，对参与访问的模块进行检查，根据模块的访问规则决定是否允许该访问。以往的个人防火墙只是对应用程序进行检查，而没有对所关联的dll做检查。进行模块检查，可防止木马模块注入到正常进程中访问网络。

8.5.2 瑞星个人防火墙的功能配置

瑞星个人防火墙的设置内容比较多，下面仅介绍与安全相关的主要功能及设置特点。

1. 工作状态

在如图8-10所示的“工作状态”选项卡中显示了个人防火墙的设置和当前系统状态等信息，具体如下。



图8-10 “工作状态”选项卡

（1）防火墙状态。主要内容如下。

- 当前账户。显示了瑞星防火墙使用的账户类型，单击后可以切换账户。
- 模块检查。显示模块保护的状态，单击后显示模块保护设置界面。
- 上网保护。显示了上网保护的状态，单击后显示网站访问规则设置界面。
- 工作模式。防火墙在当前所使用的工作模式。
- 系统漏洞。显示当前系统存在的漏洞数和不安全设置数，系统漏洞扫描时间如果超出默认设定的标准时间(例如 5 天)，显示的文字会加红显示。
- 最近操作。显示了最近一次被禁止访问网络的程序，单击该链接可转到访问规则标签页。
- 活动程序。显示了当前活动程序的图标，如果程序繁忙，对应的图标就会闪烁，用户可以轻松查看繁忙(单位时间内流量最大)的应用程序。单击该链接可转到“系统状态”选项卡下的网络活动页面。

（2）受攻击信息。可以显示攻击的名称，攻击者的 IP 地址，攻击的时间，攻击次数和攻击的端口等信息。

- 追踪位置。可以打开 http://www.ikaka.com 网站查询，根据攻击者的 IP 地址查询所在地。
- 更多信息。可以查看防火墙日志。

（3）网络状态。主要显示了如下内容。

- 流量曲线。显示接收/发送数据包流量的曲线图。其中，在曲线的左侧可以设定可显示的接收、发送数据包曲线的最高峰值；在流量曲线的右侧显示了接收、发送总的数据流量。

（4）安全级别。可拖动“工作状态”选项卡右下角的安全级别滑块到对应位置进行安全级别的设置。关于安全级别的定义及规则如下。

- 普通。系统在信任的网络中，除非规则禁止的，否则全部放过。
- 中级。系统在局域网中，默认允许共享，但是禁止一些较危险的端口。
- 高级。系统直接连接 Internet，除非规则放行，否则全部拦截。

2. 规则设置

在防火墙主窗口中选择“设置”→“详细设置”→“规则设置”命令，打开如图 8-11 所示的“详细设置”对话框。在这里可以配置防火墙的过滤规则，主要包括如下内容。

（1）黑名单。可以将禁止与本机通信的计算机添加到该列表中。例如，可以将已发现的攻击本机的计算机添加到该区域中。

（2）白名单。可以将完全信任的计算机添加到该列表中，列表中的计算机对本机有完全访问权限。例如，可以将 VPN 服务器加入到该区域中。

（3）端口开关。可以打开或关闭本机上的 TCP 或 UDP 端口，允许或禁止端口中的通信。在如图 8-12 所示的“增加端口开关”对话框中可以对端口进行设置。

（4）可信区。如图 8-13 所示，通过可信区域的设置，可以对局域网和互联网(如 Internet)区别对待。用户可以进行“可信区列表”和“选择可信区服务”的设置，可以将本机可信赖的主机的 IP 地址添加到“可信区列表”中；在“选择可信区服务”下方提供了对常用服务器的访问规则，包括“允许 Ping 入/出”、“LAN 下放行对方敏感端口”和“LAN 下放行

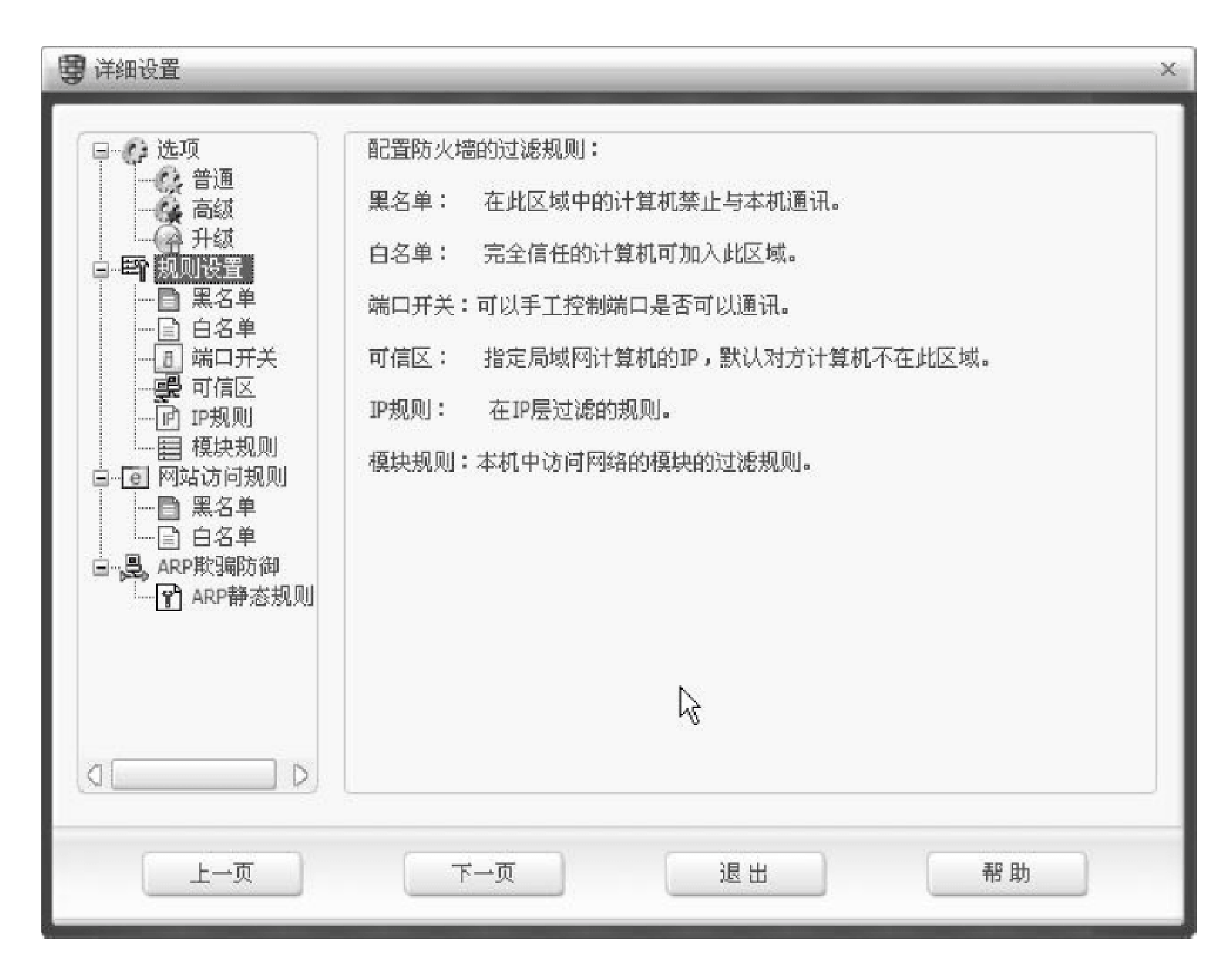


图 8-11 "详细设置"对话框



图 8-12 设置端口页面

敏感端口"三项，用户可根据实际需要进行设置。

(5) IP 规则。用于设置网络层 IP 地址的过滤规则。列表中显示了当前使用的 IP 规则，包括规则名称、状态、协议、对方端口、本地端口和是否报警等。其中，规则按过滤顺序排序，打勾的项表示生效，如图 8-14 所示。

(6) 模块规则。用户通过"模块规则"，能够控制是否允许某个模块访问网络。当应用程序访问网络的时候，防火墙对参与访问的模块进行检查，根据模块的访问规则决定是否允许该访问。如图 8-15 所示，在页面中显示了当前设置的模块名称等信息，如果要让所有的模块规则全部生效，可以选取"启动模块访问检查"复选框。如果用户需要增加规则，可以单击"增加"按钮进行设置。

3. 网站访问规则

用户通过设置网站访问规则，可以屏蔽不适合浏览的网站，给用户创建一个健康的上网环境。网站访问规则的设置页面如图 8-16 所示。



图 8-13 “可信区”设置页面



图 8-14 “IP 规则”设置页面

1）基本设置

- 启用网址过滤，防止受到钓鱼和病毒等恶意网站的侵害。如果选取此复选框，防火墙将启动上网保护功能，通过调用黑名单库，过滤钓鱼网址和病毒木马网址，防止钓鱼和病毒等恶意网站的侵害。当上网保护功能关闭后，所有的 URL 过滤功能自动关闭。
- 启用家长保护。如果选取此复选框，防火墙将启用家长保护功能。只有在启用家长保护后，所有网站访问规则才能够生效。



图 8-15 “模块规则”设置页面



图 8-16 “网站访问规则”设置页面

- 监控指定的端口。用于设置防火墙的监控端口，对用户所指定的对方网站端口进行实时监控。在用户不指定端口的情况下，防火墙默认监控 80 号端口。
- 监控代理上网。如果用户通过代理服务器上网，可选取此复选框，并设置所使用的代理服务器的信息。防火墙将会监控代理上网行为。

2）黑名单

黑名单中的网站将被禁止访问，用户可将要屏蔽的网站添加到 URL 黑名单列表中。

3）白名单

白名单中的网站不会被禁止访问，用户可将信任的网站添加到白名单列表中。

4. ARP 欺骗防御

ARP 欺骗是通过发送虚假的 ARP 数据包给局域网内的其他计算机或网关，通过冒充其他主机的身份来欺骗局域网中的其他计算机，使得其他计算机无法正常通信，或者监听被欺骗者的通信内容。用户在选取了“启用 ARP 欺骗防御”复选框后，防火墙将利用已设置的 ARP 规则来保护计算机的正常通信，如图 8-17 所示。



图 8-17 “ARP 欺骗防御”设置页面

(1) 定时检查本机 ARP 缓存。定时检查防火墙内的 ARP 缓存表和系统的 ARP 缓存表，并将两者进行比较。默认每 60s 检查一次，用户也可以重新设置时间间隔。

(2) 启用 ARP 静态地址绑定规则。选取此复选框后，用户设置的 ARP 静态地址绑定规则才生效。

(3) 拒绝 IP 地址冲突攻击。选取此复选框后，当防火墙检测到局域网中计算机的 IP 地址发生冲突时，会自动阻止所受的攻击并将所受攻击事件记录到日志中。

(4) 发现可疑或欺骗 ARP 包时如何提示用户。用户可以选择“气泡通知”、“托盘动画”和“声音报警”三种方式来通知 ARP 欺骗的发生。如果选取“记录日志”，防火墙会记录下 ARP 欺骗事件。

另外，防火墙会自动搜集局域网中各计算机的 IP 地址与 MAC 地址的对应表，当发现地址有冲突时，会出现如图 8-18 所示的提示信息。单击“添加到 ARP 静态表中”链接，防火墙



图 8-18 发现 ARP 包内容有地址冲突时的提示信息

会将用户选择的地址(其中正确的地址)添加到 ARP 静态表中。

以上简要介绍了瑞星防火墙的安全功能及安全规则的设置方法,其他功能的介绍和应用可参阅相关的技术文档。

8.6 实验操作 2 Cisco PIX 防火墙基础配置实例

虽然 Cisco PIX 防火墙的部分配置命令与 Cisco 交换机和路由器不同,但还有相当一部分命令是相同的,所以对于熟悉 Cisco 交换机和路由器配置的读者来说,学习 PIX 防火墙的配置要相应容易一些。

8.6.1 PIX 防火墙的管理访问模式

PIX 防火墙提供了 4 种管理访问模式。

(1) 非特权模式。PIX 防火墙开机自检后就处于这种模式。系统显示为 pixfirewall>(其中 pixfirewall 为防火墙的名称)。PIX 防火墙的非特权模式相当于 Cisco 交换机和路由器的用户模式。

(2) 特权模式。在非特权模式下输入 enable 命令,将进入特权模式。在特权模式下可以改变当前配置。特权模式的显示为 pixfirewall#。

(3) 配置模式。在特权模式下输入 configure terminal 命令将进入配置模式,绝大部分系统配置都在配置模式下进行。配置模式的显示为 pixfirewall(config)#。

(4) 监视模式。PIX 防火墙在开机或重启过程中,按住管理机上的 Escape 键或发送 Break 字符,将进入监视模式。在监视模式下可以更新系统映像文件,并可以进行口令的恢复操作。监视模式下的显示为 monitor>。

8.6.2 PIX 防火墙的基本配置命令

PIX 防火墙的配置命令很多,最常使用的有 6 个基本命令:nameif、interface、ip address、nat、global 和 route。下面分别对这 6 个命令的功能和使用方法进行介绍。

1. 配置防火墙接口的名称(nameif)

可以使用 nameif 命令来配置防火墙的接口名称,同时在使用 nameif 命令配置防火墙名称的时候还需要为接口指定安全等级。

```
Pix525(config)#nameif ethernet0 outside security 0   (将外网接口 ethernet 0 的安全等级设置为 0)
Pix525(config)#nameif ethernet1 inside security 100  (将内网接口 ethernet 1 的安全等级设置为 100)
Pix525(config)#nameif dmz security 50                (将 DMZ 接口的安全等级设置为 50)
```

需要注意的是,在 PIX 防火墙的默认配置中,快速以太网接口 0(ethernet 0)被命名为外部接口(outside),安全等级是 0;快速以太网 1(ethernet 1)被命名为内部接口(inside),安全等级为 100。其他安全等级的取值范围为 1~99,数字越大安全级别越高。如果添加新的接口,语句可以这样写:

```
Pix525(config)#nameif pix/interface3 security40 (安全等级设置为 40)。
```

2. 配置以太网接口参数(interface)

下面将 PIX 防火墙上的以太网接口 0(ethernet 0)配置为自适应,将以太网接口 1(ethernet 1)配置为全双工。

```
Pix525(config)# interface ethernet0 auto          (auto 选项表示该接口为自适应)
Pix525(config)# interface ethernet1 100full       (100full 选项表示该接口为 100Mbit/s 全双工)
```

如果要关闭该接口,可以使用以下命令:

```
Pix525(config)# interface ethernet1 100full shutdown (shutdown 选项表示关闭这个接口,若启用接口去掉 shutdown )
```

3. 配置内外网接口的 IP 地址(ip address)

根据系统规划,由于 PIX 防火墙还担负着路由器的功能,所以必须给相应的连接外网和内网的接口配置 IP 地址。在下面的方案中,把与外网连接的 ethernet0 接口的 IP 地址配置为 218.94.97.125,子网掩码为 255.255.255.224;将与内网连接的 ethernet1 接口的 IP 地址配置为 172.16.1.2,子网掩码为 255.255.255.0。

```
Pix525(config)# interface ethernet0               (进入接口 ethernet0 的配置状态)
Pix525(config-if)# ip address outside 218.94.97.125 255.255.255.224
Pix525(config)# interface ethernet1               (进入接口 ethernet1 的配置状态)
Pix525(config-if)# ip address inside 172.16.1.2 255.255.255.0
```

4. 进行地址转换(nat)

网络地址转换(nat)的作用是将内网的私有 IP 地址转换为外网的公有 IP 地址,nat 命令总是与 global 命令一起使用,这是因为 nat 命令可以指定一个 IP 地址或一段 IP 地址访问外网,访问外网时需要利用 global 所指定的地址池进行对外访问。nat 命令的配置格式为:

```
nat (interface_name) nat_id local_ip [netmark]
```

其中(interface_name)表示内网接口名称,多使用 inside; nat_id 用来标识全局地址池,使它与其相应的 global 命令相匹配; local_ip 表示内网被分配的 IP 地址; 0.0.0.0 表示内网所有主机可以对外访问; [netmark]表示内网 IP 地址的子网掩码。

例 1 让内网的所有主机都可以访问外网。

```
Pix525(config)# nat (inside) 1 0 0
```

也可以写成:

```
Pix525(config)# nat (inside) 1 0.0.0.0 0.0.0.0
```

其中,用 0 可以代表 0.0.0.0。

例 2 只允许 172.16.10.0/24 这个网段内的主机可以访问外网。

```
Pix525(config)# nat (inside) 1 172.16.10.0 255.255.255.0
```

5. 指定外部地址范围(global)

global 命令把内网的 IP 地址翻译成外网的一个或一段 IP 地址。global 命令的配置格式为:

```
global (interface_name) nat_id ip_address-ip_address [netmark global_mask]
```

其中,(interface_name)表示外网接口名字,一般为 outside; nat_id 用来标识全局地址池,使它与其相应的 nat 命令相匹配; ip_address-ip_address 表示转换后的单个 IP 地址或一段 IP 地址; [netmark global_mask]表示全局 IP 地址的网络掩码。下面举例说明 global 命令的功能和使用方法。

例 3 当内网的主机访问外网时,将使用 58.193.128.1～58.193.128.254 这段 IP 地址池为要访问外网的主机分配一个全局 IP 地址。

```
Pix525(config)#global (outside) 1 58.193.128.1～58.193.128.254
```

例 4 当内网要访问外网时,访问外网的所有主机统一使用 58.193.128.1 这个单 IP 地址。

```
Pix525(config)#global (outside) 1 58.193.128.1
```

当要取消配置时,像 Cisco 路由器和交换机的配置一样,只需要在命令行前面加 no 即可,如例 5 所示。

例 5 取消对 global (outside) 1 58.193.128.1 命令的配置。

```
Pix525(config)#no global (outside) 1 58.193.128.1
```

6. 配置静态路由(route)

静态路由是最常使用的一种路由选择方法,在中小型网络中尤其常见。PIX 防火墙配置静态路由的语法格式为:

```
route (interface_name) 0 0 gateway_ip [metric]
```

其中(interface_name)表示接口名称,内网接口常用 inside,外网接口常用 outside; gateway_ip 表示网关 IP 地址; [metric]表示到 gateway_ip 的跳数,通常默认是 1,0 表示 0.0.0.0。

例 6 设置一条指向 218.94.97.125 的静态路由。

```
Pix525(config)#route outside 0 0 218.94.97.125
```

该命令还可以写成:

```
Pix525(config)#route outside 0.0.0.0 0.0.0.0 218.94.97.125 1
```

以上命令,一般是指所有内部主机都通过 218.94.97.125 将数据包转发出去。

如果内部网络使用多个 IP 网段时,需要为每一个网段指定一个静态路由,例如内部网络使用了 192.168.1.0/24 和 172.16.0.0/16 两个网段,这时需要在 PIX 防火墙上同时配置以下两条静态路由,网关 IP 地址都为 218.94.97.125。

```
Pix525(config)#route inside 192.168.1.0 255.255.255.0 218.94.97.125 1
Pix525(config)#route inside 172.16.0.0 255.255.0.0 218.94.97.125 1
```

通过对以上 6 个基本命令的学习,希望读者掌握 PIX 防火墙的基本配置方法,这些命令的使用也会为后面命令的学习奠定基础。

8.6.3 PIX 防火墙的扩展配置命令

这里所讲的扩展配置命令是相对于前面的基本配置命令而言的。这些命令主要有 static、conduit、fixup 和 Telnet 等。

1. 配置静态 IP 地址转换(static)

在企业网络中,经常要提供一些诸如 Web、FTP 和 Mail 等服务,既允许内网用户,也允许外网用户访问。其中,内网用户访问时使用内部私有的 IP 地址,而外网用户访问时则需要使用公网的 IP 地址,而 static 命令的功能是进行内、外网 IP 地址之间的一对一转换。如果从外网发起一个连接请求,而请求的目的地址是一个内网的 IP 地址时,static 就把内部地址转换成一个指定的全局地址,允许这个请求建立。static 命令的配置格式为:

```
static (internal_interface_name,external_interface_name) outside_ip_address inside_ ip_
address [netmask mask]
```

其中,internal_interface_name 表示内部网络的接口名称,一般为 inside,属于高安全等级的接口;external_interface_name 表示外部网络接口的名称,一般为 outside,接口安全等级较低;outside_ip_address 为外网接口(external_interface_name)的 IP 地址;inside_ip_address 为内部网络接口(internal_interface_name)的 IP 地址;netmask 参数后面跟 mask 指定的网络掩码,如果不指定 netmask 时,将使用 IP 地址的默认掩码。

由于在通常情况下,internal_interface_name 内部网络的接口名称一般为 inside,而 external_interface_name 外部网络接口的名称为 outside,所以 static 命令也常写成如下格式:

```
static (inside,outside) outside_ip_address inside_ ip_address
```

例 7 内部主机 172.16.1.2 对于通过 PIX 防火墙建立的每个请求连接,都被转换成公网的 218.94.97.125 这个全局地址。

```
Pix525(config)# static (inside, outside) 218.94.97.125 172.16.1.2
```

Static 命令也可以理解为建立内部 IP 地址(如例 7 的 172.16.1.2)与外部 IP 地址(如例 7 的 218.94.97.125)之间的静态映射。

例 8 将 DMZ 接口的内部 IP 地址 172.16.1.10 转换为外部的 218.94.97.126 这个全局地址。

```
Pix525(config)# static (dmz, outside) 172.16.1.10 218.94.97.126
```

以上两个例子说明,使用 static 命令可以为一个特定的内部 IP 地址指定一个永久的全局 IP 地址。这样就能够为具有较低安全级别的指定接口创建一个入口,使它们可以进入到具有较高安全级别的指定接口,从而实现 Internet 的用户通过防火墙访问内部主机上的资源。

2. 管道命令(conduit)

前面讲过使用 static 命令可以在两个 IP 地址之间创建一个静态转换,但此时从外部到内部接口的连接仍然会被 PIX 防火墙的适应性安全算法(ASA)阻挡。

conduit 命令允许数据流从具有较低安全等级的接口流向具有较高安全等级的接口,例

如允许从外网接口到 DMZ 接口或内网接口的请求连接。对于向内部接口的连接，static 和 conduit 命令将一起使用来创建连接的建立。conduit 命令配置格式为：

```
conduit permit | deny global_ip port[-port] protocol foreign_ip [netmask]
```

其中，*permit*|*deny* 表示允许或拒绝访问；global_ip 所指的是先前由 global 或 static 命令定义的全局 IP 地址，如果 global_ip 为 0，就用 any 代替 0，如果 global_ip 是一台主机，就用 host 命令参数；port 表示服务所作用的端口，例如 www 使用 80，ftp 使用 21 等。可以通过服务名称或端口号来指定端口；protocol 表示连接协议，如 TCP、UDP 和 ICMP 等；foreign_ip 表示可访问 global_ip 的外部 IP 地址。对于任意主机，可以使用 any 表示。如果 foreign_ip 是一台主机，就用 host 命令参数。

下面用几个实例介绍 conduit 命令的使用方法。

例 9 允许任何外部主机对全局地址 218.94.97.125 的这台主机进行 http 访问。

```
Pix525(config)#conduit permit tcp host 218.94.97.125 eq www any
```

其中使用 eq 和一个端口或服务来允许或拒绝对这个端口的访问。eq ftp 就是指允许或拒绝只对 ftp 的访问。对于 TCP 和 UDP，可以使用操作符 eq(等于)、neq(不等于)、gt(大于)、lt(小于)或者是一个 range(范围)进行设置。

例 10 不允许外部主机 58.128.15.99 对任何全局地址进行 FTP 访问。

```
Pix525(config)#conduit deny tcp any eq ftp host 58.128.15.99
```

例 11 表示允许 ICMP 消息通过 PIX 防火墙(系统默认情况下 ICMP 消息是不允许通过 PIX 防火墙的)。

```
Pix525(config)#conduit permit icmp any any
```

例 12 通过 static 和 conduit 命令，实现外网的所有用户能够通过防火墙访问 Web 服务器(内部 IP 地址为 172.16.1.2，外部 IP 地址为 218.94.97.125)。

```
Pix525(config)#static (inside, outside) 218.94.97.125 172.16.1.2
Pix525(config)#conduit permit tcp host 218.94.97.125 eq www any
```

在这个例子中，先用 static 命令实现内部私有 IP 地址 172.16.1.2 与外网全局地址 218.94.97.125 之间的转换，然后利用 conduit 命令允许任何外部主机对全局地址 218.94.97.125 进行 http 访问。

3. 启用或禁止协议(fixup)

fixup 命令的作用是启用或禁止某一协议，从而决定某一个服务或协议是否允许通过 PIX 防火墙。由 fixup 命令指定的端口是 PIX 防火墙要侦听的对象。下面举例进行说明。

例 13 启用 FTP 协议，并指定 FTP 服务的端口号为 21。这样内网用户将可以利用 21 号端口来访问外网的 FTP 资源。

```
Pix525(config)#fixup protocol ftp 21
```

例 14 为 http 协议指定 80 和 8080 两个端口。

```
Pix525(config)#fixup protocol http 80
Pix525(config)#fixup protocol http 8080
```

4. 设置远程登录(Telnet)

PIX 防火墙操作系统的版本在 5.0(OS 5.0)之前,只允许从内部网络上的主机通过 Telnet 远程登录防火墙。在 OS 5.0 及后续版本中,对远程登录的主机开始不再进行限制,凡是与 PIX 防火墙连接的主机经配置后都可以 Telnet 到 PIX 防火墙。

不过,当从外网接口 Telnet 到 PIX 防火墙时,Telnet 数据流需要用 IPSec 协议提供保护,也就是说用户必须在 PIX 防火墙上配置一条到另外一台主机(如 PIX 防火墙、路由器和客户端等)的 IPSec 通道。另一种方法是在 PIX 防火墙上配置 SSH,然后用 SSH Client 从外部主机 Telnet 到 PIX 防火墙。PIX 防火墙同时支持 SSH1 和 SSH2,不过 SSH1 是免费软件,SSH2 是商业软件。这里仅介绍只允许内部网络的主机 Telnet 到 PIX 防火墙的方法,这时的 Telnet 配置格式为:

```
Telnet local_ip [netmask] local_ip
```

例 15 配置仅允许内部网络 172.16.1.0/24 网段的主机 Telnet 到 PIX 防火墙。

```
Telnet 172.16.1.0 255.255.255.0 inside
```

如果不设此项,PIX 的配置方式只能通过 console 口进行。

另外,需要说明的是,当对 PIX 防火墙进行配置后,防火墙重新启动后配置会丢失,如果要让配置保存下来,需要通过 write memory 命令将其进行保存。

```
PIX525#write memory
```

习　题

8-1 试分析防病毒软件与防火墙的功能特点,并比较两者之间在应用上的不同。

8-2 结合实际应用,从用户的角度分析防火墙应具有的功能。

8-3 试分析防火墙的“所有未被允许的就是禁止的”和“所有未被禁止的就是允许的”这两条规则的特点。

8-4 试描述包过滤防火墙的工作原理,并分析包过滤防火墙的应用特点。

8-5 代理防火墙的工作原理是什么?与包过滤防火墙相比有何特点?

8-6 状态检测防火墙是如何工作的?与包过滤防火墙相比有何特点?

8-7 名词解释:企业级防火墙、个人防火墙。

8-8 与企业级防火墙相比,个人防火墙有哪些应用特点?

8-9 从计算机网络的安全现状和未来发展入手,试分析企业级防火墙和个人防火墙技术及产品的发展趋势。

8-10 选择一款个人防火墙软件(如瑞星个人防火墙软件),通过对安全规则的配置掌握个人防火墙的功能及应用特点。

8-11 通过实验掌握 PIX 防火墙的基本配置方法,以此了解企业级防火墙的功能及应用特点。

第 9 章 VPN 技术及应用

近年来,随着全球信息化建设的快速发展,对网络基础设施的功能和可延伸性提出了新的要求。例如,一些跨地区组织的各分支机构之间需要进行远距离的互联;一些单位的员工需要远程接入内部网络进行移动办公。为了解决各分支机构局域网之间的互联问题,早期只能通过直接铺设网络线路或租用运营商的专线,不但成本高,而且实现困难。对于移动办公用户来说,早期一般采用拨号方式接入到内部网络,在需要支付较高的通信费用的同时,还要考虑到通信的安全问题。VPN 技术可以在公共网络(如 Internet)中为用户建立专用的通道,为局域网之间的远程互联,以及内部网络的远程接入提供廉价和安全的方式。本章将较为系统地介绍 VPN 技术的原理及实现方法。

9.1 VPN 技术概述

VPN 不是一种独立的组网技术,它只是一组通信协议,其目的是在 Internet 等公共网络中虚拟出一条专用通道,供通道的两个端节点之间安全地传输信息。

9.1.1 VPN 的概念

VPN(Virtual Private Network,虚拟专用网)是利用 Internet 等公共网络的基础设施,通过隧道技术,为用户提供一条与专用网络具有相同通信功能的安全数据通道,实现不同网络之间及用户与网络之间的相互连接。IETF 草案对基于 IP 网络的 VPN 的定义为:使用 IP 机制仿真出一个私有的广域网。

从 VPN 的定义来看,其中“虚拟”是指用户不需要建立自己专用的物理线路,而是利用 Internet 等公共网络资源和设备建立一条逻辑上的专用数据通道,并实现与专用数据通道相同的通信功能;“专用网络”是指这一虚拟出来的网络并不是任何连接在公共网络上的用户都能够使用的,而是只有经过授权的用户才可以使用。同时,该通道内传输的数据经过了加密和认证,从而保证了传输内容的完整性和机密性。由此可以看出,VPN 不是一个物理意义上的专用网络,但它却具有与物理专用网络相同的功能。

从实现方法来看,VPN 是指依靠 ISP(Internet Service Provider,Internet 服务提供商)和 NSP(Network Service Provider,网络服务提供商)的网络基础设施,在公共网络中建立专用的数据通信通道。在 VPN 中,任意两个节点之间的连接并没有传统的专用网络所需的端到端的物理链路。只是在两个专用网络之间或移动用户与专用网络之间,利用 ISP 和 NSP 提供的网络服务,通过专用 VPN 设备和软件,根据需求构建永久的或临时的专用通道。图 9-1(a)所示的是 VPN 的物理拓扑,其功能等价于 9-1(b)所示的逻辑拓扑。

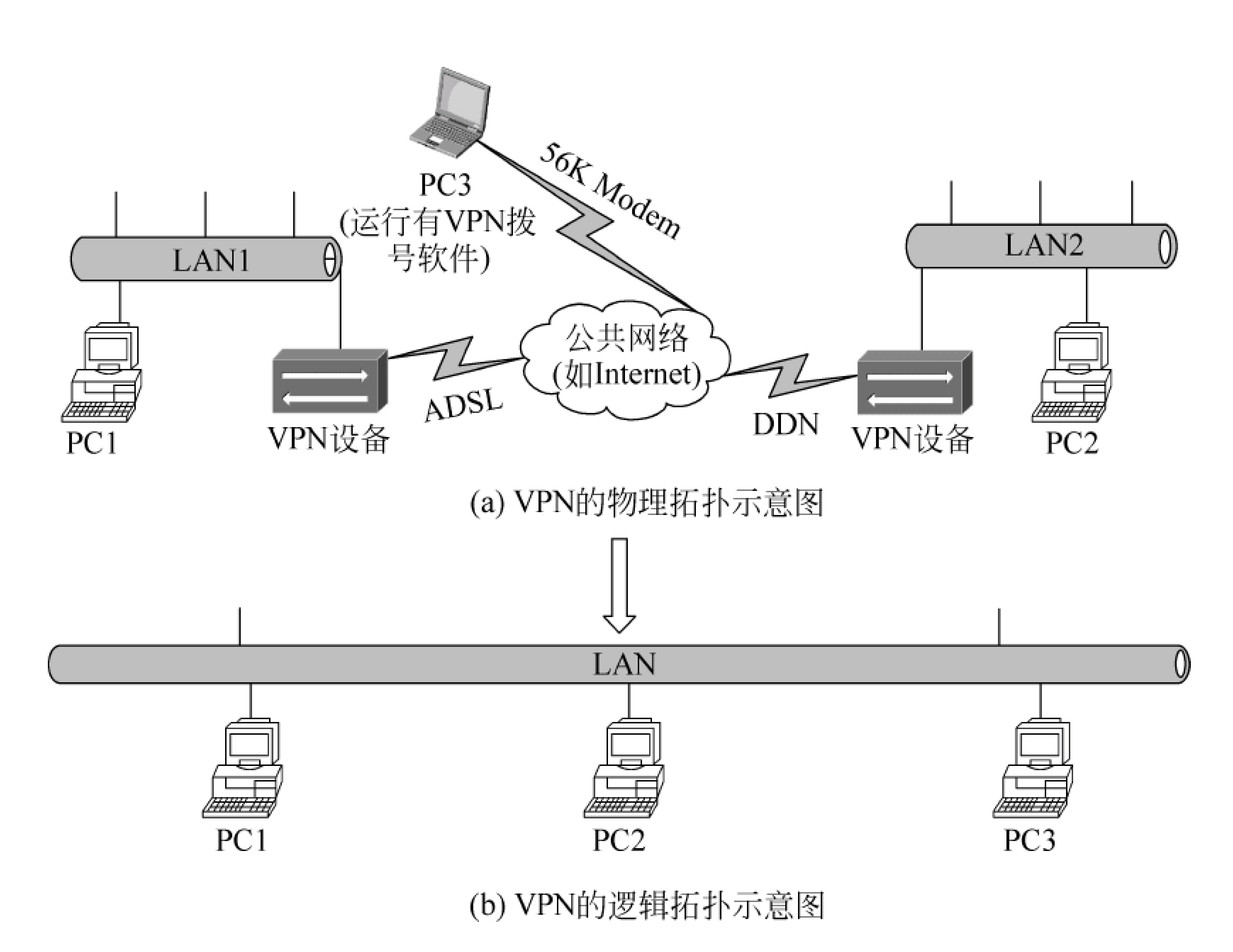


图 9-1 VPN 组成示意图

9.1.2 VPN 的基本类型及应用

根据应用环境的不同,VPN 主要分为三种典型的应用方式:内联网 VPN、外联网 VPN 和远程接入 VPN。

1. 内联网 VPN

内联网 VPN(Intranet VPN)的组网方式如图 9-2 所示。这是一种最常使用的 VPN 连接方式,它将位于不同地址位置的两个内部网络(LAN1 和 LAN2)通过公共网络(主要为 Internet)连接起来,形成一个逻辑上的局域网。位于不同物理网络中的用户在通信时,就像在同一局域网中一样。

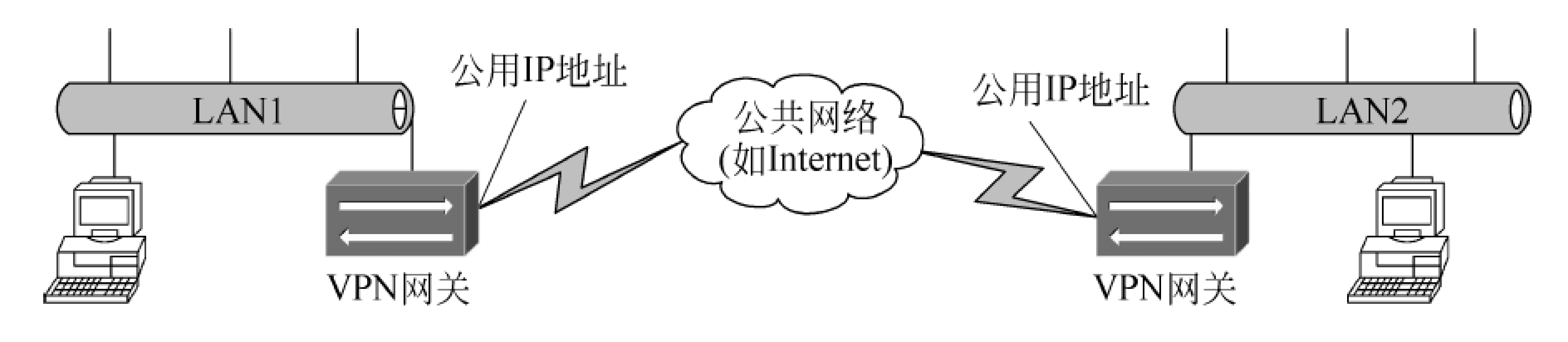


图 9-2 内联网 VPN 连接示意图

在内联网 VPN 未使用之前,如果要实现两个异地网络之间的互联,就必须直接铺设网络线路,或租用运营商的专线。不管采用哪一种方式,使用和维护成本都很高,而且不便于网络的扩展。在使用了内联网 VPN 后,可以很方便地实现两个局域网之间的互联,其条件是分别在每一个局域网中设置一台 VPN 网关,同时每一个 VPN 网关都需要分配一个公用 IP 地址,以实现 VPN 网关的远程连接。而局域网中的所有主机都可以使用私有 IP 地址进行通信。图 9-2 所示的是两个局域网之间通过 VPN 的远程互联方式,根据用户需求也可以实现多个局域网之间的远程互联。

目前,许多具有多个分支机构的组织在进行局域网之间的互联时,多采用内联网 VPN 这种方式。

2. 外联网 VPN

外联网 VPN(Extranet VPN)的组网方式如图 9-3 所示。与内联网 VPN 相似,外联网 VPN 也是一种网关对网关的结构。在内联网 VPN 中位于 LAN1 和 LAN2 中的主机是平等的,可以实现彼此之间的通信。但在外联网 VPN 中,位于不同内部网络(LAN1、LAN2 和 LAN3)的主机在功能上是不平等的。

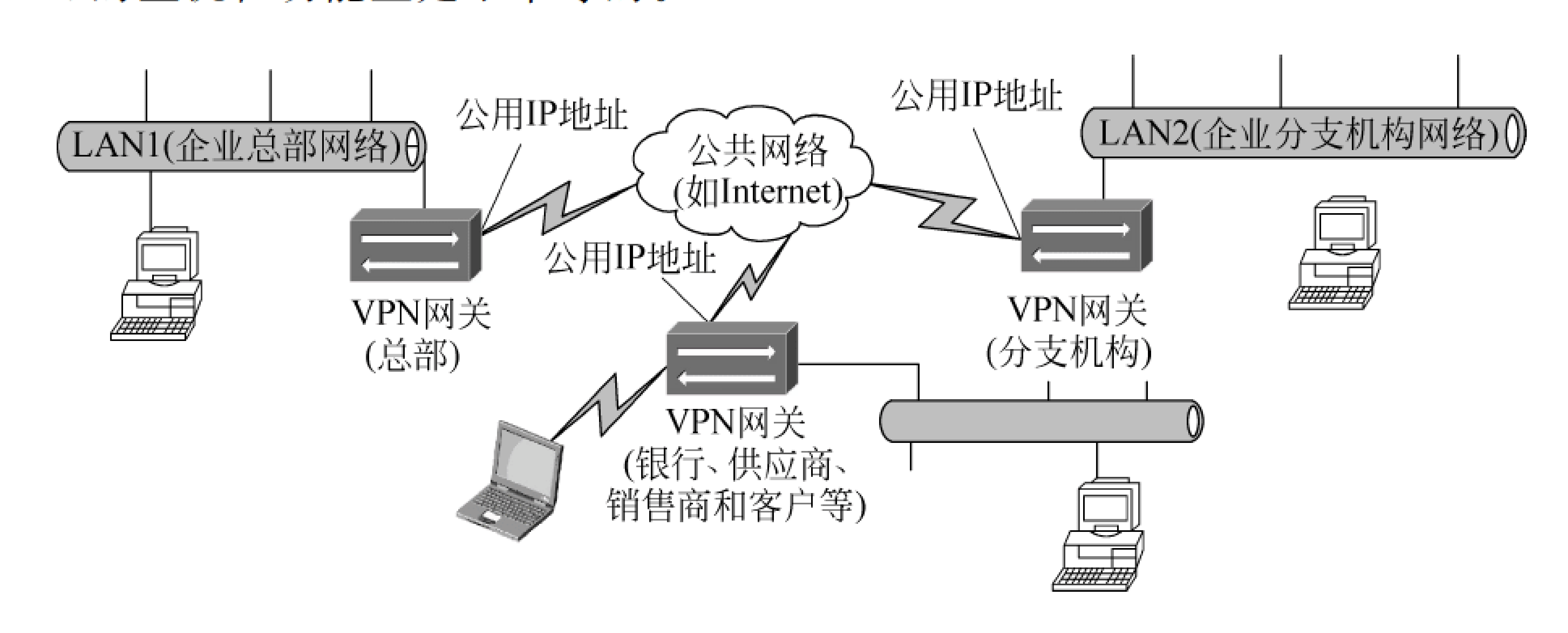


图 9-3 外联网 VPN 连接示意图

外联网 VPN 是随着企业经营方式的发展而出现的一种网络连接方式。现代企业需要在企业与银行、供应商、销售商及客户之间建立一种联系(即电子商务活动),但是在这种联系过程中,企业需要根据不同的用户身份(如供应商、销售商等)进行授权访问,建立相应的身份认证机制和访问控制机制。

外联网 VPN 其实是对内联网 VPN 在应用功能上的延伸,是在内联网 VPN 的基础上增加了身份认证、访问控制等安全机制。

3. 远程接入 VPN

远程接入 VPN(Access VPN)的组网方式如图 9-4 所示。远程接入 VPN 也称为移动 VPN,即为移动用户提供一种访问单位内部网络资源的方式,主要应用于单位内部人员在外(非内部网络)访问单位内部网络资源的情况下,或为家庭办公的用户提供远程接入单位内部网络的服务。

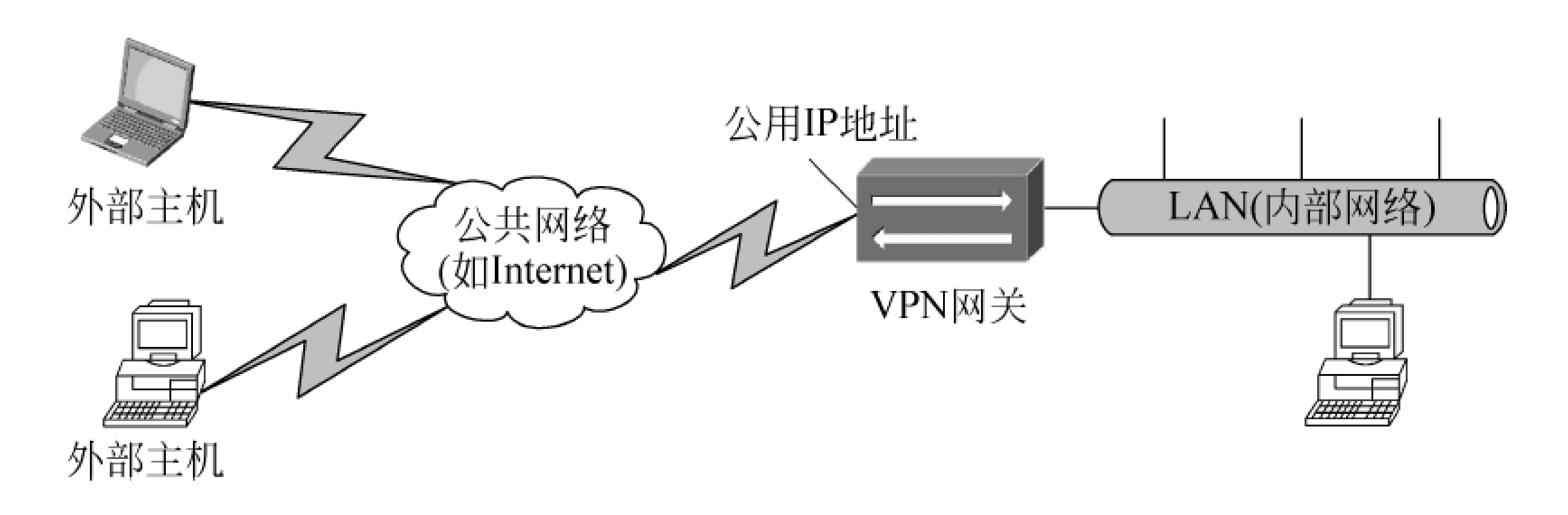


图 9-4 远程接入 VPN 连接示意图

在远程接入 VPN 技术出现之前,如果用户要通过 Internet 连接到单位内部网络,需要在单位内部网络中部署一台远程访问服务器(Remote Access Server,RAS),用户通过拨号方式连接到该 RAS 后再根据相应权限来访问内部网络中的相应资源。远程拨号方式需要

RAS 的支持，而且用户与 RAS 之间的通信是以明文方式进行，缺乏安全性。另外，远程的拨号用户可能需要支持长途电话通信费。而远程接入 VPN 方式中的远程用户，只需要通过当地的 ISP 接入到 Internet 就可以连接到单位的 VPN 网关，并访问单位内部的资源。与传统的远程拨号方式相比，远程连接 VPN 方式实现容易，使用费用较低。简单来说，只要用户能够接入 Internet，就可以使用远程接入 VPN 方式连接到单位内部网络。

目前，远程接入 VPN 方式的使用非常广泛，许多企业和高校都采用这种方式为本单位用户提供访问内部网络资源的服务。例如，现在许多高校都建有内部的数字资源数据库，如中国期刊全文数据库、电子图书馆和学位论文数据库等。考虑到安全和版权等问题，对这些数据库系统的访问权限进行了限制，一般只允许本单位内部的用户在内部局域网中使用。为了方便本单位用户在外部网络中能够访问单位内部的网络资源，许多高校都部署了远程访问 VPN 系统。

9.1.3 VPN 的实现技术

VPN 是在 Internet 等公共网络基础上，综合利用隧道技术、加密技术和身份认证技术来实现的。

1. 隧道技术

隧道(Tunneling)技术是 VPN 的核心技术，它是利用 Internet 等公共网络已有的数据通信方式，在隧道的一端将数据进行封装，然后通过已建立的虚拟通道(隧道)进行传输。在隧道的另一端，进行解封装操作，将得到的原始数据交给对端设备。

在进行数据封装时，根据在 OSI 参考模型中位置的不同，可以分为第二层隧道技术和第三层隧道技术两种类型。其中，第二层隧道技术是在数据链路层使用隧道协议对数据进行封装，然后再把封装后的数据作为数据链路层的原始数据，并通过数据链路层的协议进行传输。第二层隧道协议主要有：

- L2F(Layer 2 Forwarding，主要在 RFC 2341 文档中进行了定义)
- PPTP(Point-to-Point Tunneling Protocol，主要在 RFC 2637 文档中进行了定义)
- L2TP(Layer 2 Tunneling Protocol，主要在 RFC 2661 文档中进行了定义)

第三层隧道技术是在网络层进行数据封装，即利用网络层的隧道协议将数据进行封装，封装后的数据再通过网络层的协议(如 IP)进行传输。第三层隧道协议主要有：

- IPSec(IP Security，主要在 RFC 2401 文档中进行了定义)
- GRE(Generic Routing Encapsulation，主要在 RFC 2784 文档中进行了定义)

有关隧道技术的详细内容在本章随后进行专门介绍。

2. 加密技术

通过 Internet 等公共网络传输的重要数据必须经过加密处理，以确保网络上其他未授权的实体无法读取该信息。目前在网络通信领域中常用的信息加密体制主要包括对称加密体制和非对称加密体制两类。实际应用时一般是将对称加密体制和非对称加密体制混合使用，利用非对称加密技术进行密钥的协商和交换，而采用对称加密技术进行用户数据的加密。

在 VPN 解决方案中最普遍使用的对称加密算法主要有 DES、3DES、AES、RC4、RC5 和 IDEA 等算法。使用的非对称加密算法主要有 RSA、Diffie-Hellman 和椭圆曲线等。有

关加密算法和密钥管理的相关内容已在本书的第 2 章和的第 3 章进行了介绍。

3. 身份认证技术

VPN 系统中的身份认证技术包括用户身份认证和信息认证两个方面。其中,用户身份认证用于鉴别用户身份的真伪,而信息认证用于保证通信双方的不可抵赖性和信息的完整性。从实现技术来看,目前采用的身份认证技术主要分为非 PKI 体系和 PKI 体系两类,其中非 PKI 体系主要用于用户身份认证,而 PKI 体系主要用于信息认证。

其中非 PKI 体系一般采用"用户 ID+密码"的模式,目前在 VPN 系统中采用的非 PKI 体系的认证方式主要有如下几种。

(1) PAP(Password Authentication Protocol,密码认证协议)。PAP 是一种不安全的身份验证协议。当使用 PAP 时,客户端的用户账号名称和对应的密码都以明文形式进行传输。由于采用了未加密的明文传输方式,所以 PAP 协议存在不安全性。

(2) CHAP(Challenge-Handshake Authentication Protocol,询问握手认证协议)。CHAP 会将客户端用户的密码采用标准的 MD5 算法进行加密处理,然后再发送给服务器端。所以,CHAP 要比 PAP 和 SPAP 安全。

(3) EAP(Extensible Authentication Protocol,扩展身份认证协议)。EAP 允许用户根据自己的需要来自行定义认证方式。EAP 的使用非常广泛,它不仅用于系统之间的身份认证,而且还用于有线和无线网络的验证。除此之外,相关厂商可以自行开发所需要的 EAP 认证方式,例如视网膜认证、指纹认证等都可以使用 EAP。

(4) MS-CHAP(Microsoft Challenge Handshake Authentication Protocol,微软询问握手认证协议)。MS-CHAP 是微软公司针对 Windows 系统来设计的,它是采用 MPPE(Microsoft Point-to-Point Encryption)加密方法将用户的密码和数据同时进行加密后再发送。

(5) SPAP(Shiva Password Authentication Protocol,Shiva 密码认证协议)。SPAP 是针对 PAP 的不足而设计的,当采用 SPAP 进行身份认证时,SPAP 会加密从客户端发送给服务器端的密码,所以 SPAP 比 PSP 安全。

(6) RADIUS(Remote Authentication Dial In User Service,远程用户认证拨号系统),相关内容已在本书的第 4 章进行了介绍。

PKI 体系主要通过 CA,采用数字签名和 Hash 函数保证信息的可靠性和完整性。例如,目前用户普遍关注的 SSL VPN 就是利用 PKI 支持的 SSL 协议实现应用层的 VPN 安全通信。有关 PKI 的内容已在本书的第 3 章进行了介绍。

9.1.4 VPN 的应用特点

由于 VPN 技术具有非常明显的应用优势,所以近年来 VPN 产品引起了企业用户的普遍关注,各类纯软件平台的 VPN、专用硬件平台的 VPN 及集成到网络设备(主要为防火墙)中的 VPN 产品不断推出,而且在技术上推陈出新,以满足不同用户的应用需求。

1. VPN 的应用优势

对于企业用户来说,VPN 提供了基于 Internet 的安全、可靠和廉价的远程访问通道,具有以下的应用优势。

(1) 节约成本。VPN 的实现是基于 Internet 等公共网络的,用户不需要单独铺设专用

的网络线路(如铺设光纤等),也不需要向 ISP 或 NSP 租用专线(如 DDN、光纤和虚电路等),只需要连接到当地的 ISP 就可以安全地接入单位内部网络,节省了网络建设、使用和维护成本。

(2) 提供了安全保障。VPN 综合利用数据加密和身份认证等技术,保证了通信数据的机密性和完整性,使信息不被泄露或暴露给未经授权的用户。

(3) 易于扩展。如果同一组织的不同局域网之间采用专线连接,不但费用昂贵,而且不便于扩展和维护。如果采用 VPN 方式,则只需要在每一个 LAN 中增加一台 VPN 设备,就可以利用 Internet 建立安全连接,配置和维护比较简单,费用较低。

2. VPN 存在的不足

VPN 存在的不足主要是安全问题。VPN 扩展了网络的安全边界。例如,在局域网出口处设置了 VPN 网关(如图 9-4 所示)后,网络的安全边界将由局域网扩展到外部主机。如果外部主机的安全比较脆弱,那么入侵者可以利用外部主机连接到 VPN 网关后进入内部网络。另外,VPN 系统中密钥的产生、分配、使用和管理,以及用户身份的认证方式都会影响 VPN 系统的安全性。

在实际应用中,一种有效的安全解决方案是除建立完善的加密和身份认证机制外,还需要将 VPN 和防火墙配合应用,通过防火墙增加 VPN 系统的安全性。

9.2 VPN 的隧道技术

VPN 技术是网络安全领域继防火墙之后出现的一项安全技术,它的技术核心是隧道技术,VPN 的加密和身份认证等安全技术都需要与隧道技术相结合来实现。

9.2.1 VPN 隧道的概念

网络隧道(Tunneling)技术的核心内容是指利用一种网络协议(该协议称为隧道协议)来传输另一种网络协议。在面向非连接的公共网络上建立一个逻辑的、点对点连接的过程称为建立了一个隧道。目前,隧道技术在计算机网络中的应用非常广泛,除本章介绍的 VPN 隧道外,隧道技术在 IPv4 与 IPv6 互联等应用领域大量使用。隧道有多种实现方式,本章主要介绍基于 IP 网络的 VPN 隧道技术。

1. 隧道的组成

要形成隧道,需要有以下几项基本的要素。

(1) 隧道开通器(TI)。隧道开通器的功能是在公共网络中创建一条隧道。

(2) 有路由能力的公用网络。由于隧道是建立在公共网络中,要实现 VPN 网关之间或 VPN 客户端与 VPN 网关之间的连接,这一公共网络必须具有路由功能。

(3) 隧道终止器(TT)。隧道终止器的功能是使隧道到此终止,不再继续向前延伸。

2. 隧道的实现过程

图 9-5 所示的是一个基于 IP 网络的 VPN 隧道,通过隧道将 LAN1 和 LAN2 连接起来,使位于 LAN1 和 LAN2 中的主机之间可以像在同一网络中一样利用 IP 进行通信。为了便于对隧道的工作过程进行描述,现假设与 LAN1 连接的 VPN 网关为隧道开通器,而与 LAN2 连接的 VPN 网关为隧道终止器,用户数据从 LAN1 发往 LAN2,具体过程如下。

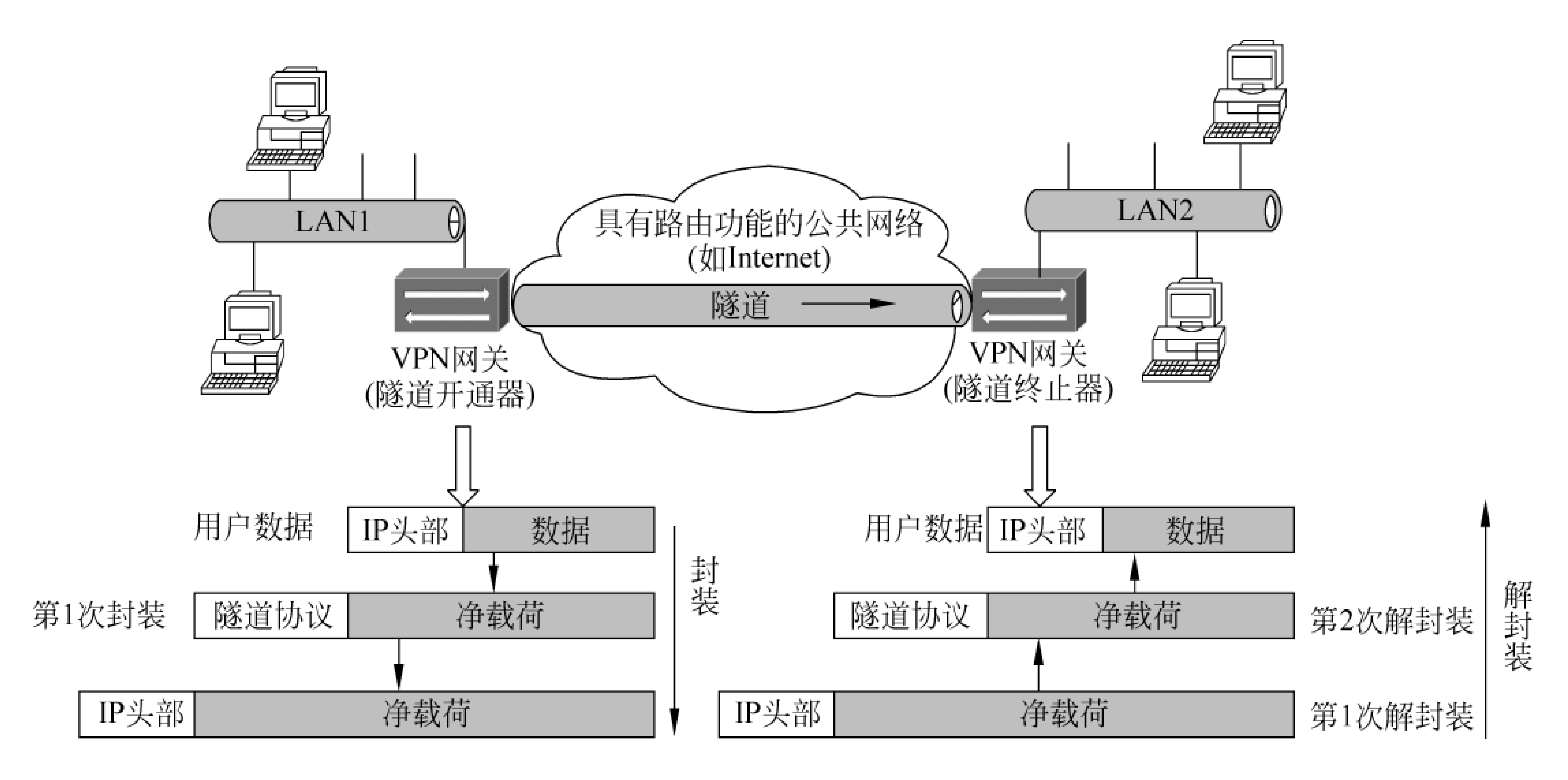


图 9-5　隧道的工作原理示意图

(1) 封装。封装操作发生在隧道开通器上。当用户数据(包括有 IP 头部和数据两部分)到达隧道开通器时,隧道开通器将用户数据作为自己的净载荷,并对该净载荷利用隧道协议进行第 1 次封装。这一次封装其实是利用隧道协议对上层数据(用户数据)进行加密和认证处理。

第 1 次封装后形成的数据成为第 2 次封装的净载荷。为了使第 1 次封装后的数据能够通过具有路由功能的公共网络(如 Internet)进行传输,还需要给它添加一个 IP 头部,即进行第 2 次封装。第 2 次封装后的数据根据其 IP 头部信息进行路由选择,并传输到与 LAN2 连接的 VPN 网关。

(2) 解封装。解封装操作发生在隧道终止器上。解封装操作是封装操作的逆过程,第 1 次解封装去掉最外层用于在公共网络中进行寻址的 IP 头部信息,第 2 次解封装去掉隧道协议,最后得到的是用户数据。用户数据再根据其头部信息在 LAN2 中找到目的主机,完成通信过程。

在数据封装过程中,虽然出现了两个"IP 头部",但用户数据中的"IP 头部"在隧道中是不可见的,即在隧道中传输时主要依靠第 2 次封装时添加的"IP 头部"信息进行路由寻址。所以,用户数据中的"IP 头部"对隧道来说是透明的。

3. 隧道的功能

从以上隧道的工作原理可以看出,隧道通过封装和解封装操作,只负责将 LAN1 中的用户数据原样传输到 LAN2,使 LAN2 中的用户感觉不到数据是通过公共网络传输过来的。通过隧道的建立,可实现以下功能。

(1) 将数据流量强制传输到特定的目的地。虽然隧道建立在公共网络上,但是由于在隧道的两个端点(如 VPN 网关)之间建立了一条虚拟的通道,所以从隧道一端进入的数据只能被传输到隧道的另一端。

(2) 隐藏私有的网络地址。在如图 9-5 所示的 VPN 连接中,LAN1 和 LAN2 中的主机一般使用私有 IP 地址(用户数据中的"IP 头部"),只有 VPN 网关使用公用 IP 地址(第 2 次封装添加的"IP 头部")。隧道的功能就是在隧道开通器和隧道终止器之间建立一条专用通

道，私有网络之间的通信内容经过隧道开通器封装后通过公共网络的虚拟专用通道进行传输，然后在隧道终止器上进行解封装操作，还原成私有网络的通信内容，并转发到私有网络中。这样对于两个使用私有 IP 地址的私有网络来说，公共网络就像普通的通信电缆，而接在公共网络上的 VPN 网关则相当于两个特殊的节点。

(3) 在 IP 网络上传输非 IP 协议的数据包。隧道只需要连接两个相同类型(使用相同的通信协议)的网络，至于这两个网络内部使用什么类型的通信协议，隧道并不关心。对于隧道开通器来说，不管接收到的是什么类型的数据，都会对它进行封装，然后通过隧道传输到另一端的隧道终止器，由隧道终止器通过解封装操作进行还原。所以，可以在 IP 网络上通过建立隧道来传输 IPX/SPX、NetBEUI 和 Appletalk 等任何一类协议的数据。

(4) 提供数据安全支持。由于在隧道中传输的数据是经过加密和认证处理的，从而可以保证这些数据在传输中的安全性。

概括地讲，隧道技术是一种在公共网络基础设施上建立的端到端数据传输方式。使用不同协议(如 TCP/IP、IPX/SPX、NetBEUI 和 Appletalk 等)的用户数据都可以在隧道中传输。首先隧道协议将这些用户数据进行重新封装，然后再在重新封装后的数据上添加一个头部。头部提供了路由信息，从而使封装的数据能够通过具有路由功能的公共网络进行传输。

9.2.2 隧道的基本类型

根据隧道建立方式的不同，可分为主动式隧道和被动式隧道两种基本类型。

1. 主动式隧道

当一个客户端计算机利用隧道客户端软件主动与目标隧道服务器建立一个连接时，该连接称为主动式隧道。在主动式隧道的建立过程中，需要在客户端计算机上安装所需要的隧道协议，并且能够通过 Internet 等公共网络连接到隧道服务器。如图 9-6(a)所示，如果客户端计算机是通过 Internet 拨号方式建立与隧道服务器的连接，需要以下三个步骤的操作。

(1) 客户端计算机可以拨号连接到当地的 ISP，建立一个到 Internet 的连接。

(2) 在客户端计算机上利用隧道客户端软件与隧道服务器之间建立隧道。在此过程中，客户端计算机首先要知道隧道服务器的 IP 地址(或主机名)，同时在隧道服务器上已经为该客户端创建了连接账户，并分配了访问内部网络资源的相应权限。

(3) 将客户端的 PPP 帧(用户数据)进行封装，通过隧道传送到目的地。

这是一种最为常用的隧道建立方式。对于专线接入 ISP 的用户，由于客户端计算机本身已经建立到 Internet 的连接，则免去了以上的第(1)步操作，可以直接建立起与隧道服务器的连接，然后进行数据的传输。

Access VPN 中用户与 VPN 网关之间的隧道建立一般采用主动式隧道。

2. 被动式隧道

被动式隧道的工作过程类似于如图 9-6(b)所示的结构。在主动式隧道模式中，客户端计算机根据需要与隧道服务器之间建立临时的隧道。与主动式隧道不同的是，被动式隧道主要用于两个内部网络(LAN1 与 LAN2)之间的固定连接。所以，当 LAN1 中的某一客户端计算机需要与 LAN2 中的计算机进行通信时，数据全部被交给隧道服务器 A。隧道服务器 A 在接收到该数据后，将其强制通过已建立的隧道传输到对端的隧道服务器 B。与主动

式隧道的另一个不同是，被动式隧道可以被多个客户端共享，而主动式隧道只能供建立该隧道的客户端计算机独立使用。

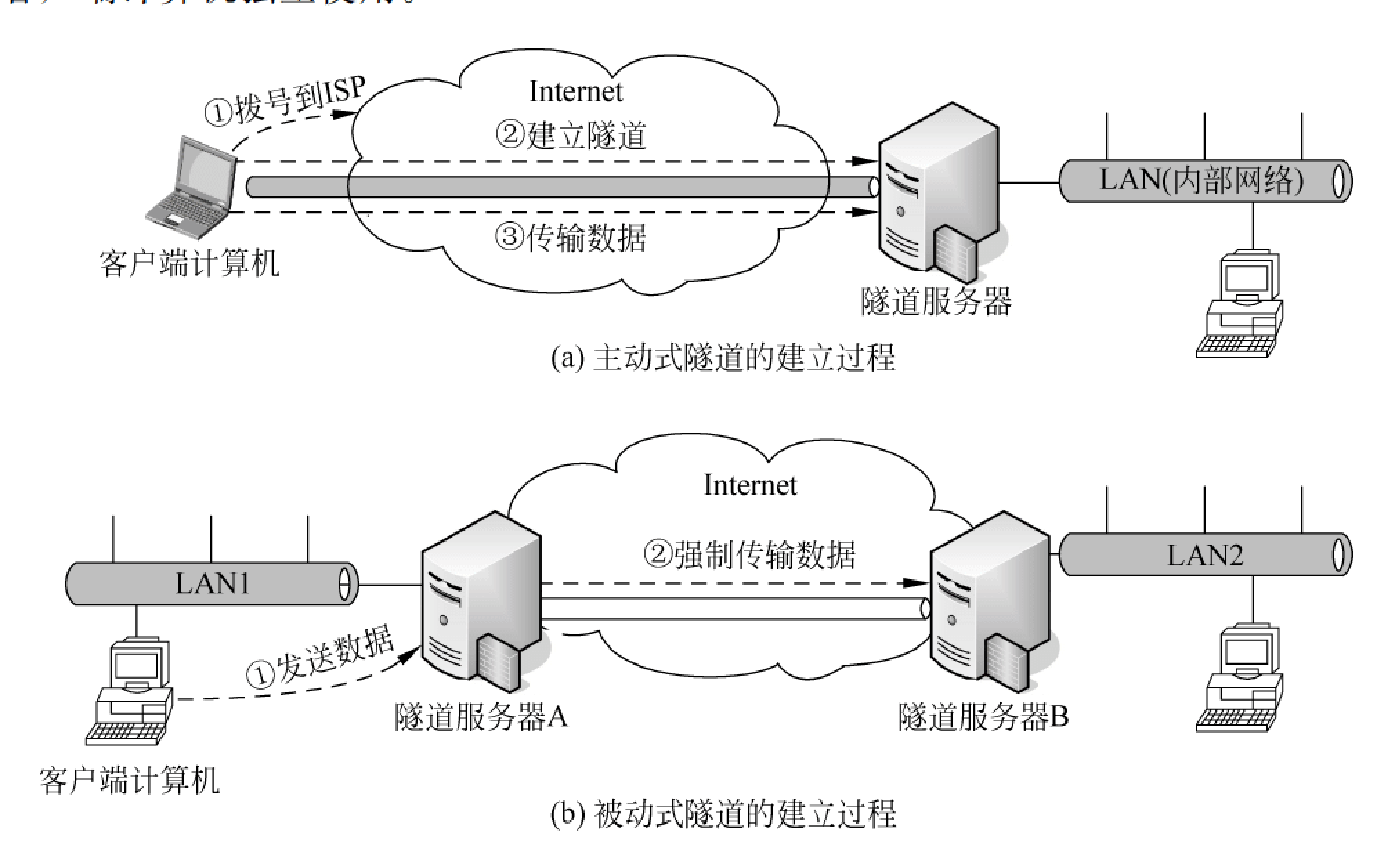


图 9-6　隧道的建立过程

在被动式隧道中，两个内部网络之间的隧道在用户传输数据之前就已经建立，所有发往另一个内部网络的用户数据都自动地汇集到已建立的隧道中传输。所以，被动式隧道也称为强制式隧道。

Intranet VPN 和 Extranet VPN 中，VPN 网关之间的隧道属于被动式隧道。

9.3　实现 VPN 的第二层隧道协议

第二层隧道协议是在 OSI 参考模型的第二层（数据链路层）实现的隧道协议。由于数据链路层的数据单位称为帧，所以第二层隧道协议是以帧为数据交换单位来实现的。用于实现 VPN 的第二层隧道协议主要有 PPTP、L2TP 和 L2F。

在具体介绍相关协议之前，需要对第二层协议的功能进行说明。第二层协议的实现依靠的是设备的物理地址（如网卡的 MAC 地址），负责在两个直连的设备之间进行数据交换。所以，下面所介绍的第二层隧道协议都是一种以物理寻址为基础的点对点的数据传输方法。

9.3.1　PPTP

PPTP（Point-to-Point Tunneling Protocol，点对点隧道协议）是建立在 PPP（Point-to-Point）协议和 TCP/IP 协议之上的第二层隧道协议。PPTP 实际上是对 PPP 协议的一种扩展，它在 PPP 的基础上增强了认证、压缩和加密等功能，提高了 PPP 协议的安全性。PPTP 协议是一个第二层的隧道协议，它提供了 PPTP 客户端与 PPTP 服务器之间的加密通信，允许在公共 IP 网络（如 Internet）上建立隧道。PPTP 支持 TCP/IP、IPX/SPX、Appletalk 和 NetBEUI 等多种网络协议。

1. PPP

由于 PPTP 是在 PPP 基础上发展起来的，所以在介绍 PPTP 之前对 PPP 进行简要的介绍。PPP 是 Internet 中使用的一个点对点的数据链路层协议，其目的是在 TCP/IP 网络中的一个物理节点实现对上层数据(IP 数据报)的封装，然后通过已确定的物理链路将封装后的数据发送到下一个物理节点。在下一个物理节点进行解封装操作后，将封装前的数据(IP 数据报)提供给该节点的上一层(网络层)进行处理。为此，PPP 的主要功能是在 TCP/IP 网络中实现两个相邻物理节点(路由器或计算机)之间的通信，它只负责在两个物理节点之间"搬运"上层数据，并不关心上层数据的具体内容。

2. PPTP 的工作过程

微软公司是 PPTP 协议的主要发起者，所以 Windows 操作系统都支持 PPTP 协议。PPTP 中创建的隧道属于主动式隧道，一般由 PPTP 客户机发起隧道建立连接请求，在得到 PPTP 服务器认证后才能建立隧道。

PPTP 提供了在 IP 网络中建立多协议的安全 VPN 的通信方式，远端用户能够通过任何支持 PPTP 的 ISP 访问企业内部网络。PPTP 提供了 PPTP 客户机与 PPTP 服务器之间的安全通信。其中，PPTP 客户机是指运行 PPTP 协议的计算机，而 PPTP 服务器是指运行 PPTP 协议的服务器。通过 PPTP，客户机可以采用 PSTN、ISDN、xDSL、以太网和无线等连接，以拨号方式接入公共 IP 网络。拨号客户机首先按正常的网络接入方式拨号到 ISP 的网络接入服务器(NAS)，建立 PPP 连接。在此基础上，客户机进行第二次拨号建立到 PPTP 服务器的连接，该连接称为 PPTP 隧道。PPTP 隧道实质上是基于 IP 协议的另一个 PPP 连接，其中 IP 数据报可以封装成 TCP /IP、IPX/SPX 和 NetBEUI 等多种协议数据。如果客户机是直接接入到本地局域网，而且本地局域网已连接到 IP 网络，这时客户机则不需要第一次的 PPP 拨号连接，可以直接与 PPTP 服务器建立隧道。

对于基于 PPTP 的 VPN 而言，由于客户机是通过拨号方式接入到 VPN 服务器，所以该 VPN 服务器也称为 VPDN(Virtual Private Dial-up Network，虚拟专用拨号网)服务器。下面以 Windows 操作系统为例，介绍基于 PPTP 协议的 VPN 的实现过程。如图 9-7 所示，基于 PPTP 协议的 VPN 是一种客户机/服务器的结构，包括 PPTP 服务器(VPDN 服务器)和 PPTP 客户机两部分。具体工作过程如下。

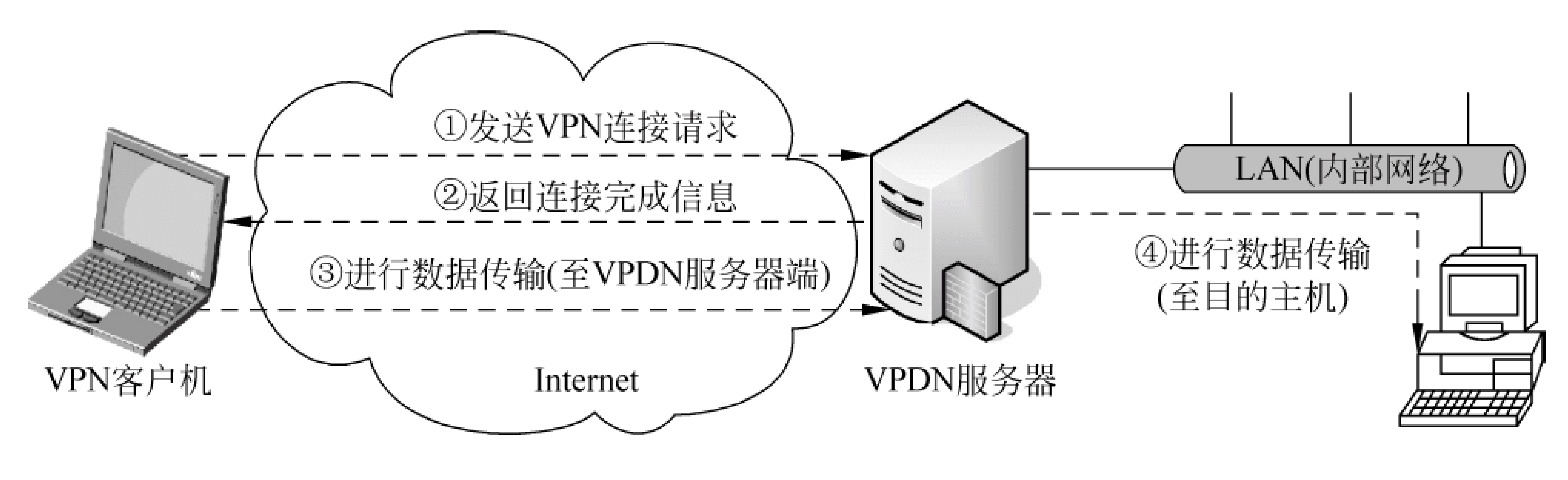


图 9-7 基于 PPTP 隧道的 VPN 的工作示意图

(1) 发送建立连接请求。在此之前，需要在 VPDN 服务器端为 PPTP 客户机建立好用户账户(包括登录账号和对应的密码)。PPTP 客户机向 VPDN 服务器发起连接请求，具体可利用客户端 VPN 连接软件来实现(Windows 操作系统自带)。在输入 VPDN 服务器的

IP 地址后，首先要将登录账号和密码发送到 VPDN 服务器端进行用户认证，以防止非法用户侵入受保护的内部网络。

其中，PPTP 用户的认证可以使用多种方法，如 PAP、SPAP、CHAP、MS-CHAP 和 EAP 等。

(2) 返回连接完成信息。当 VPDN 服务器验证了用户的合法性后，返回连接完成信息，表示已经正式建立了 VPN 连接。

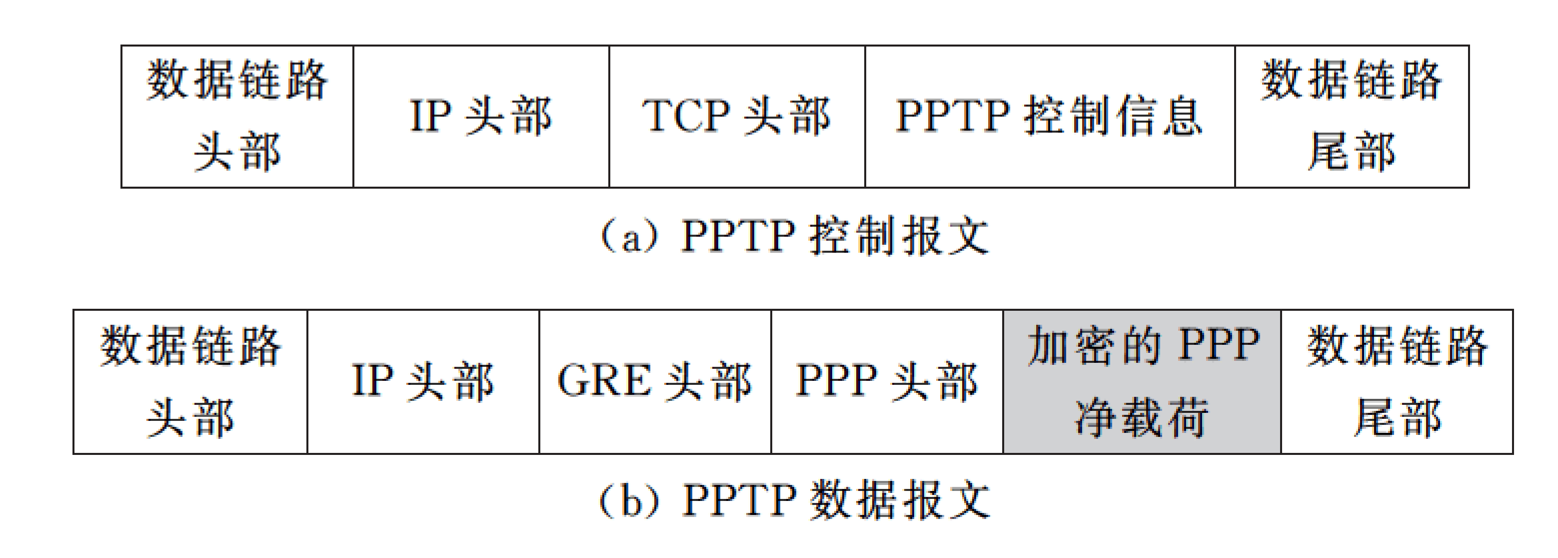
(3) 进行数据传输(至 VPDN 服务器端)。在接收到连接完成信息后，表示 VPN 安全隧道已经建立，这时就可以进行正常的数据通信。在 VPN 客户机与 VPDN 服务器之间进行数据通信时，为了保证数据传输的安全性，可以选用 MPPE、RSA 和 DES 等算法对 IP 数据报进行加密。其中，在 Windows 操作系统中多使用微软公司自己的 MPPE 算法进行数据的加密处理。

(4) 进行数据传输(至目的主机)。当 VPDN 服务器接收到远程用户机发送过来的 PPTP 数据报后开始对其进行处理。首先进行解封装操作，从 PPTP 数据报中取出本地内部网络中的计算机的 IP 地址(私有 IP 地址)或计算机名称信息，然后根据此信息将其中的 PPP 数据报转发到目的主机。

3. PPTP 的报文格式

在 PPTP 客户机与 PPTP 服务器之间传输的报文分为两种类型：控制报文和数据报文。

(1) PPTP 控制报文。负责 PPTP 隧道的建立、维护和断开。当 PPTP 客户机通过第一次拨号建立了与 IP 网络的连接后，再通过第二次拨号建立与 PPTP 服务器的隧道连接。其中，第二次拨号通过 PPTP 客户机上的 PPTP 拨号软件(使用 TCP 动态端口)与 PPTP 服务器的 TCP 1723 端口建立控制连接。PPTP 控制报文的结构如图 9-8(a)所示，其中各字段的内容如下。



数据链路头部	IP 头部	TCP 头部	PPTP 控制信息	数据链路尾部

(a) PPTP 控制报文

数据链路头部	IP 头部	GRE 头部	PPP 头部	加密的 PPP 净载荷	数据链路尾部

(b) PPTP 数据报文

图 9-8　PPTP 报文格式

- IP 头部。标明参与隧道建立的 PPTP 客户机和 PPTP 服务器的 IP 地址及其他相关信息。
- TCP 头部。标明建立隧道时使用的 TCP 端口等信息，其中 PPTP 服务器的端口为 TCP 1723。
- PPTP 控制信息。携带了 PPTP 呼叫控制和管理，用于建立和维护 PPTP 隧道。
- 数据链路头部和数据链路尾部。用数据链路层协议对连接数据包(IP 头部、TCP 头部和 PPTP 控制信息)进行封装，从而实现相邻物理节点之间的数据包传输。

PPTP 控制连接的建立过程如下。

① 在 PPTP 客户机上动态分配的 TCP 端口(1024 以上)与 PPTP 服务器上的 TCP 1723 端口之间建立一个 TCP 连接。

② PPTP 客户机发送一个用以建立 PPTP 控制连接的 PPTP 消息。

③ PPTP 服务器向 PPTP 客户机返回一条 PPTP 消息,对连接请求进行响应。

④ PPTP 客户机在接收到 PPTP 服务器的响应后,再向 PPTP 服务器发送另一条 PPTP 消息,并且选择一个用以对从 PPTP 客户机向 PPTP 服务器发送数据的,对 PPTP 隧道进行标识的调用 ID。

⑤ 当 PPTP 服务器接收到该消息后,通过另一条 PPTP 消息进行应答。并且为自己选择一个用以对从 PPTP 服务器向 PPTP 客户机发送数据的,对 PPTP 隧道进行标识的调用 ID。

⑥ PPTP 客户机发送一条 PPTP Set-Link-Info 消息,以便指定 PPP 协商选项。

(2) PPTP 数据报文。负责传输用户的数据,其报文结构如图 9-8(b)所示。在利用 PPTP 控制报文完成隧道的建立后,初始的用户数据(如 TCP/IP 数据报、IPX/SPX 数据报文或 NetBEUI 数据帧等)经过加密后,形成加密的 PPP 净载荷。然后,添加 PPP 头部信息,封装形成 PPP 帧;PPP 帧再进一步添加 GRE 头部信息,经过第二次封装便形成 GRE 报文;第三次封装将添加 IP 头部信息,其中 IP 头部信息包含数据包的源 IP 地址和目的 IP 地址;数据链路层封装是对 IP 数据报文根据网络连接的情况,添加相应的数据链路头部和数据链路尾部信息。

在进行第二次封装时使用了 GRE(Generic Routing Encapsulation,通用路由封装)协议。当通过 PPTP 连接发送数据时,PPP 帧将利用 GRE 协议进行封装,其中 GRE 头部信息中包含了用以对数据包所使用的特定 PPTP 隧道进行标识的信息。有关 GRE 的详细内容将在本章随后的内容中进行介绍。

当 PPTP 服务器接收到 PPTP 数据包时,通过以下过程进行解封装过程操作。

① 处理并去掉数据链路层头部和尾部信息。

② 处理并去掉 IP 头部信息。

③ 处理并去掉 GRE 和 PPP 头部信息。

④ 如果需要的话,对 PPP 有效净载荷(即用户数据)进行解密或解压缩处理,具体根据 PPTP 客户机对用户数据的处理情况而定。

⑤ 对用户数据进行接收或转发处理。

9.3.2 L2TP

L2TP(Layer 2 Tunneling Protocol,第二层隧道协议)是由 Cisco、Ascend、Microsoft、3Com 和 Bay 等厂商共同制定,1999 年 8 月公布了 L2TP 的标准 RFC 2661。

1. L2TP 的组成

L2TP 是典型的被动式隧道协议,它结合了 L2F 和 PPTP 的优点,可以让用户从客户机或接入服务器端发起 VPN 连接。L2TP 是把链路层 PPP 帧封装在公共网络设施(如 IP、ATM、帧中继和 X.25 等)中进行隧道传输的封装协议。本章仅介绍基于 IP 网络的 L2TP。

L2TP 主要由 LAC(L2TP Access Concentrator,L2TP 接入集中器)和 LNS(L2TP Network Server,L2TP 网络服务器)构成。

(1) LAC。支持客户端的 L2TP,用于发起呼叫、接收呼叫和建立隧道。LAC 要求具有 PPP 端系统和 L2TP 协议处理功能,一般是一个 NAS(Network Access Server,网络接入服务器),为用户提供通过 PSTN、ISDN 和 xDSL 等多种方式接入网络的服务。

(2) LNS。是所有隧道的终点。在正常的非使用隧道的 PPP 连接中,用户拨号连接的终点是 LAC,而 L2TP 将 PPP 连接的终点延伸到 LNS。LNS 一般是一台能够处理 L2TP 服务器端协议的主机。

2. L2TP 的特点

在安全性方面考虑,L2TP 对传输中的数据(控制报文和数据报文)并不加密,所以 L2TP 并不能满足用户对安全性的需求。为了消除 L2TP 协议的安全隐患,在实际应用中可以使用 IPSec 安全协议对 L2TP 控制报文和 L2TP 数据报文提供安全保护。所以,在部署基于 L2TP 的 VPN 系统时,一般都通过 IPSec 加强系统的安全性。

L2TP 解决了多个 PPP 链路的捆绑问题。L2TP 隧道建立在 LAC 和 LNS 之间,在同一对 LAC 和 LNS 之间可以建立多个 L2TP 隧道,同时在同一个 L2TP 隧道中可以绑定多个 PPP 链路。这是因为 L2TP 头部信息中包含有隧道标识(Tunneling ID)和会话标识(Session ID),分别用来识别不同的隧道和会话,可以将隧道标识相同而会话标识不同的多个 PPP 链路复制到同一条隧道中。隧道标识在建立隧道时被分配,而会话标识是在隧道建立后分配并用于传输用户数据。

3. L2TP 的工作过程

L2TP 的建立过程如下(如图 9-9 所示)。

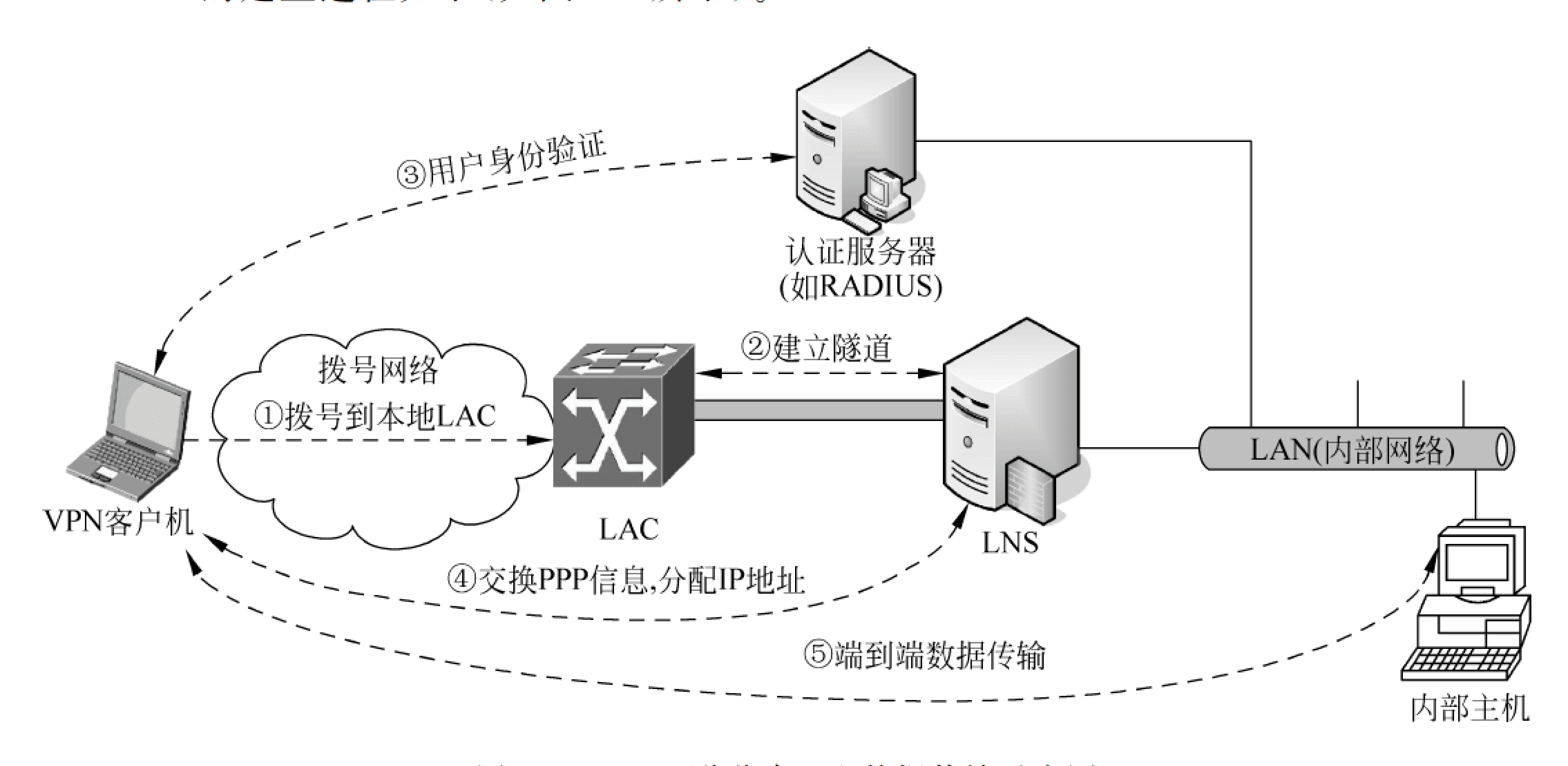


图 9-9　L2TP 隧道建立和数据传输示意图

(1) 用户通过 PSTN、ISDN 和 xDSL 等拨号方式连接到本地接入服务器 LAC,LAC 接收呼叫并进行基本的辨别。其中辨别方式可以采用域名、呼叫线路识别(CLID)或拨号 ID 业务(DNIS)等。

(2) 当用户被确认为合法用户时,就建立一个通向 LNS 的拨号 VPN 隧道。

(3) 位于内部网络中的安全认证服务器(如 RADIUS 服务器)对拨号用户的身份进行鉴别。

(4) LNS与远程用户交换PPP信息,并分配IP地址。LNS分配给远程用户的IP地址由管理人员设置,既可以是公共IP地址,也可以是私有IP地址。在实际应用中一般使用私有IP地址,因为LNS分配的IP地址将通过网络服务提供商(NSP)的公共IP网络在PPP帧内传送,LNS分配的IP地址对NSP来说是透明的。其中,LAC和LNS需要使用公共IP地址。

(5) 端到端的数据从拨号用户传到LNS。在实际应用中,LAC将拨号用户的PPP帧封装后,传送到LNS,LNS去掉封装的头部信息得到PPP帧,再去掉PPP帧的头部信息,得到网络层的用户数据。

4. L2TP的报文格式

L2TP客户机与LNS之间的报文也有两种:控制报文和数据报文。与PPTP不同的是,L2TP的两种报文采用UDP来封装和传输。下面以Windows 2000/2003操作系统中的L2TP为例,介绍基于IPSec的L2TP的报文格式。

(1) L2TP控制报文。Windows 2000/2003中使用IPSec加密的L2TP控制报文的结构如图9-10(a)所示。与PPTP一样,L2TP的控制报文用于隧道的建立、维护与断开。但与PPTP不同的是,Windows 2000/2003中的L2TP控制报文在L2TP服务器端使用了UDP 1701端口,L2TP客户端系统默认也使用UDP 1701端口,但也可以使用其他的UDP端口。另外,与PPTP不同的是,在L2TP的控制报文中,对封装后的UDP数据报使用IPSec ESP进行了加密处理,同时对使用IPSec ESP加密后的数据进行了认证。其他操作与PPTP基本相同。

数据链路头部	IP头部	IPSec ESP头部	UDP头部	L2TP控制信息	IPSes ESP尾部	IPSec ESP认证尾部	数据链路尾部

(a) Windows 2000/2003 L2TP控制报文

数据链路头部	IP头部	IPSec ESP头部	UDP头部	L2TP头部	PPP头部	加密的PPP净载荷	IPSec EPS尾部	IPSec EPS认证尾部	数据链路尾部

(b) Windows 2000/2003 L2TP数据报文

图9-10 Windows 2000/2003 L2TP报文格式

ESP是IPSec安全体系中使用的一个安全协议,主要用来处理IP数据报的加密,同时还可以实现对数据的认证等功能。有关ESP的详细内容在本章随后的内容中进行介绍。

(2) L2TP数据报文。负责传输用户的数据,其封装后的报文结构如图9-10(b)所示。下面介绍客户端L2TP数据报文的封装过程(即客户端发送L2TP数据的过程)。

① PPP封装。为PPP净载荷(如TCP/IP数据报、IPX/SPX数据报或NetBEUI数据帧等)添加PPP头部,封装成为PPP帧。

② L2TP封装。在PPP帧上添加L2TP头部信息,进行第二封装,形成L2TP帧。

③ UDP封装。在L2TP帧的头部添加L2TP客户端和L2TP服务器的UDP端口(默认为1701),将L2TP帧封装成为UDP报文。

④ IPSec封装。当L2TP使用IPSec进行加密和安全认证时,可在UDP报文的头部添加IPSec ESP头部信息,在尾部依次添加IPSec ESP尾部和IPSec ESP认证尾部信息,用于对数据的加密和安全认证。

⑤ IP 封装。在 IPSec 报文的头部添加 IP 头部信息，形成 IP 报文。其中 IP 头部信息中包含有 IPSec 客户端和 IPSec 服务器的 IP 地址。

⑥ 数据链路层封装。根据 L2TP 客户端连接的物理网络类型（如以太网、PSTN 和 ISDN 等）添加数据链路层的帧头和帧尾，完成对数据的最后封装。封装后的数据帧在链路上进行传输。

L2TP 服务器端的处理过程正好与 L2TP 客户端相反，为解封装操作，最后得到封装之前的净载荷。有效的净载荷将交付给内部网络，由内部网络发送到目的主机。

9.3.3 L2F

L2F（Layer 2 Forwarding，第二层转发）协议是由 Cisco 公司提出的可以在多种网络类型（如 ATM、帧中继和 IP 网络等）上建立多协议的安全 VPN 的通信方式。它将数据链路层的协议（如 HDLC、PPP 等）封装起来传送，所以网络的数据链路层完全独立于用户的数据链路层协议。L2F 的标准于 1998 年提交给 IETF，并在 RFC 2341 文档中发布。

1. L2F 的工作过程

以在 IP 网络中实现基于 L2F 的 VPN 为例（如图 9-11 所示），L2F 远端用户通过 PSTN、ISND 和以太网等方式拨号接入公共 IP 网络，并通过以下步骤完成隧道的建立和数据的传输。

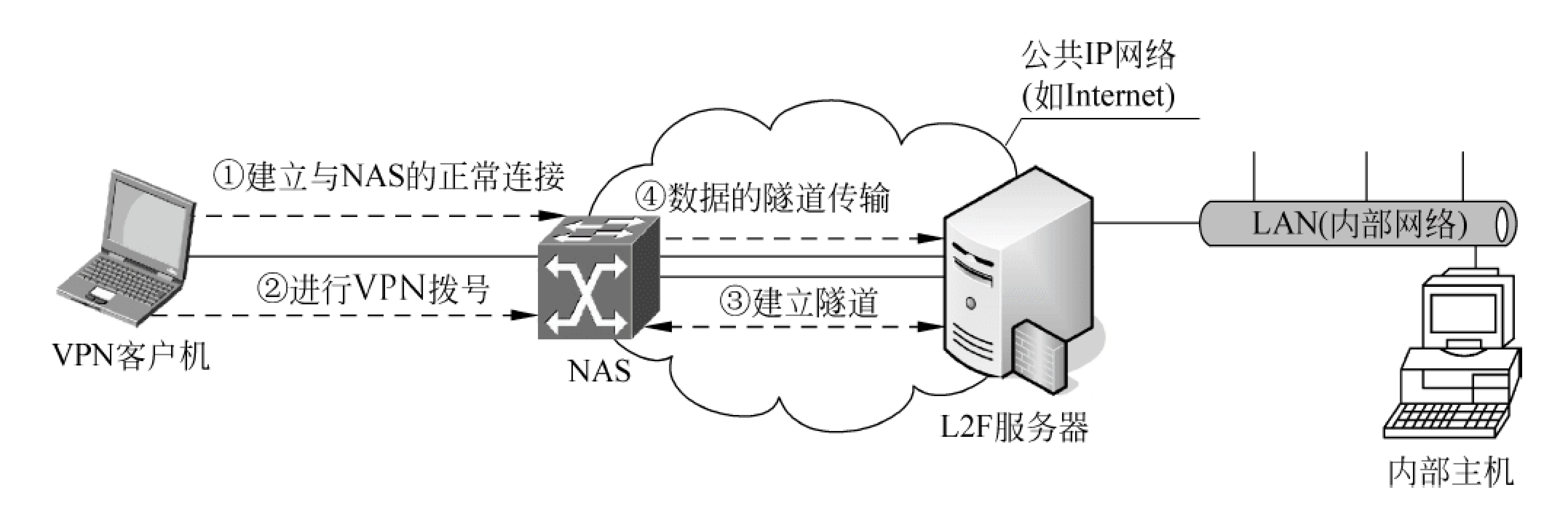


图 9-11 L2F 隧道建立和数据传输示意图

（1）建立与 NAS 的正常连接。用户按正常访问 IP 网络的方式连接到 NAS 服务器，建立 PPP 连接。

（2）进行 VPN 拨号。VPN 客户机通过 VPN 软件向 NAS 服务器发送请求，希望建立与远程 L2F 服务器的 VPN 连接。

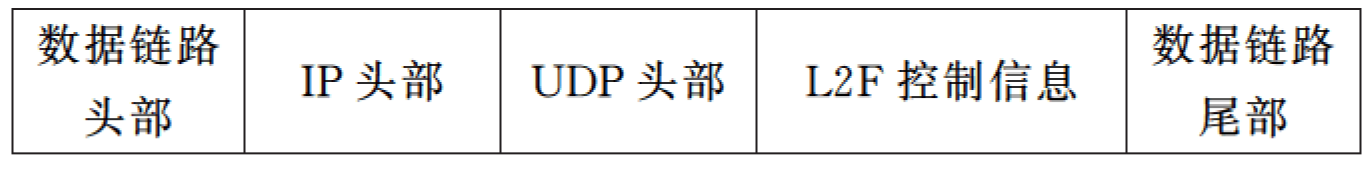
（3）建立隧道。NAS 根据用户名称等信息对远程 L2F 服务器发送隧道建立连接请求。这种方式下，隧道的配置和建立对用户是完全透明的。

（4）数据传输。L2F 服务器允许 NAS 发送 PPP 帧，并通过公共 IP 网络连接到 L2F 服务器。这时，由 VPN 客户机发送过来的数据，在 NAS 上进行 L2F 封装，然后通过已建立的隧道发送到 L2F 服务器。

L2F 服务器将接收到的报文进行解封装操作后，把封装前的用户数据（净载荷）接入到内部网络中，进一步交付给目的主机。

2. L2F 的报文格式

与 PPTP 和 L2TP 一样，L2F 的报文也分为控制报文和数据报文两部分。其中 L2F 控制报文用于 L2F 隧道的建立、维护和断开，而 L2F 数据报文负责在 L2F 隧道中进行数据的传输。L2F 控制报文和 L2F 数据报文的格式分别如图 9-12(a)和图 9-12(b)所示。



数据链路头部	IP 头部	UDP 头部	L2F 控制信息	数据链路尾部

(a) L2F 控制报文

数据链路头部	IP 头部	UDP 头部	L2F 头部	PPP 头部	加密的 PPP 净载荷	L2F 校验（可选）	数据链路尾部

(b) L2F 数据报文

图 9-12　L2F 报文格式

L2F 具备两个特殊之处：一是在进行 L2F 的封装时，增加了可选的 L2F 检验信息，以确保 L2F 数据帧的可靠传输；二是与 L2TP 相同，L2F 也使用 UDP 端口来封装 L2F 数据帧。另外，在创建 L2F 隧道的过程中，使用的认证协议为 PAP 或 CHAP。除此之外，L2F 报文格式与 L2TP 和 PPTP 类似，所以 L2F 报文的封装和解封装过程不再单独介绍。

通过前面对 PPTP、L2TP 和 L2F 协议的介绍，在隧道的整个实现过程中共存在三种不同类型的协议：乘客协议(passenger protocol)、封装协议(encapsulating protocol)和运载协议(carrier protocol)。其中，乘客协议为被封装在隧道内的协议，在第二层隧道中主要为 PPP(或 SLIP，SLIP 是 PPP 的早期协议)；封装协议用来创建、维护和断开隧道，如前面介绍的 PPTP、L2TP 和 L2F；运载协议用来运载乘客协议，它是公共网络中使用的通信协议，如 TCP/IP、IPX/SPX 和 Appletalk 等。由于 Internet 应用的广泛性，目前主要使用的运载协议为 TCP/IP。需要说明的是，运载协议与封装协议之间不存在依赖关系。

9.4　实现 VPN 的第三层隧道协议

第三层隧道协议对应于 OSI 参考模型中的第三层(网络层)，使用分组(也称为包)作为数据交换单位。与第二层隧道协议相比，第三层隧道协议在实现方式上相应要简单些。用于实现 VPN 的第三层隧道协议主要有 GRE 和 IPSec。

9.4.1　GRE

GRE(Generic Routing Encapsulation，通用路由封装)是由 Cisco 和 Net-Smiths 公司共同提出，并于 1994 提交给 IETF，分别以 RFC 1701 和 RFC 1702 文档发布。2002 年，Cisco 等公司对 GRE 进行了修订，称为 GRE v2，相关内容在 RFC 2784 中进行了规定。

1. GRE 的工作原理

如图 9-13 所示，在最简单的情况下，路由器接收到一个需要封装和路由的原始数据报文(Payload，净载荷)后，这个报文首先被 GRE 封装成 GRE 报文，接着被封装在 IP 协议中，然后完全由 IP 层负责路由寻址和转发。由此可以看出，GRE 在封装过程中不用关心原始数据包的具体格式和内容。原始数据包和 IP 头部都将成为封装后数据包的一部分。

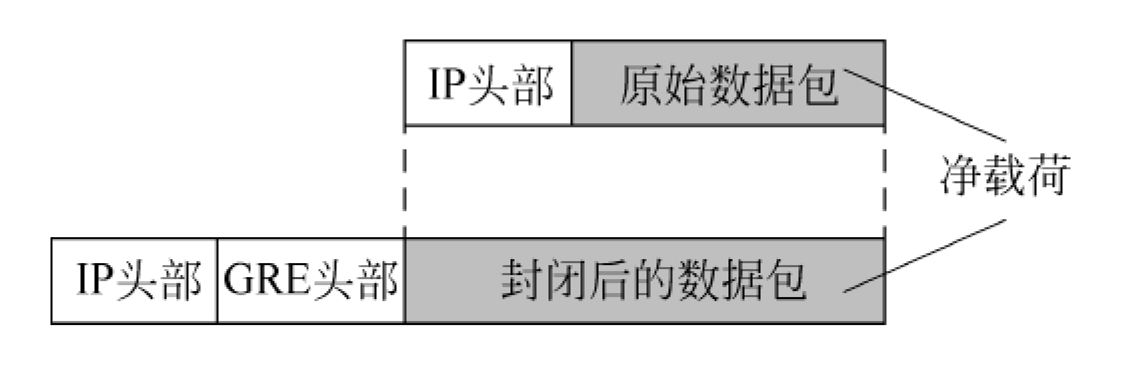


图 9-13　GRE 的报文格式

GRE 除封装 IP 报文外，还支持对 IPX/SPX、Appletalk 等多种网络通信协议的封装，同时还广泛支持对 RIP、OSPF、BGP 和 EBGP 等路由协议的封装。

隧道是一个虚拟的点对点的连接，提供了一条通路使封装的数据报文能够在这个通路上传输，并且在一个隧道的两端分别对数据包进行封装及解封装。一个第三层的报文要想在隧道中传输，必须要经过加封装与解封装两个过程，下面以图 9-14 所示的网络为例，对基于第三层隧道技术的 GRE 的封装和解封装过程进行说明。封装过程（假设数据从 IPX/SPX 网络 A 发往网络 B）如下。

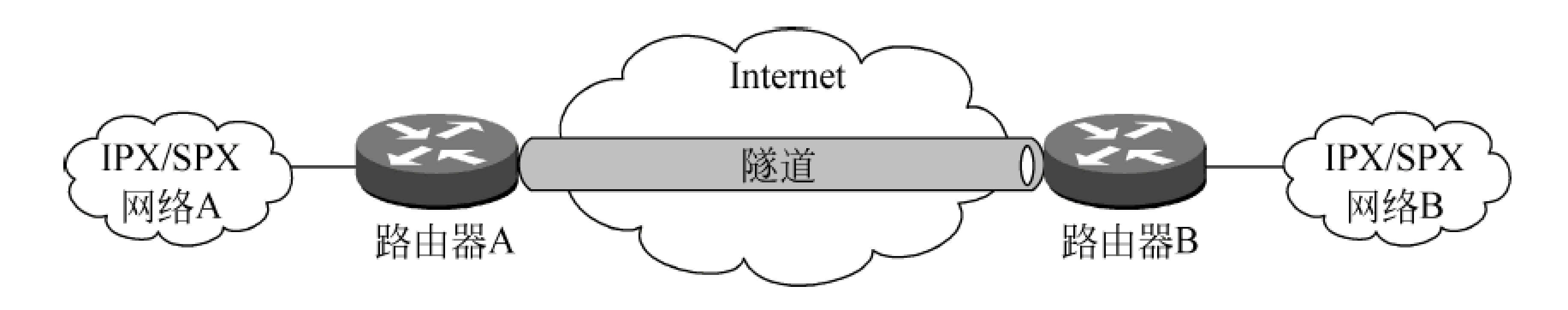


图 9-14　IPX/SPX 网络之间通过基于 Internet 的 GRE 隧道互联

（1）路由器 A 连接 IPX/SPX 网络 A，并接收从网络 A 中发过来的 IPX 报文。

（2）路由器 A 检查 IPX 报头中的目的地址，并以此来确定如何路由该报文。

（3）如果报文需要通过隧道来传输，则路由器 A 将该 IPX 报文发给路由器 A 上与隧道相连的接口。

（4）路由器 A 的隧道接口接收到此 IPX 报文后首先添加 GRE 头部信息，进行 GRE 封装。接着 IP 模块处理对 GRE 封装后的报文，进行添加 IP 头部信息，进行 IP 封装，形成新的 IP 报文。

（5）路由器 A 根据 IP 的目的地址查看自己的路由表，进行对 IP 报文的转发。

解封装是封装的逆过程，具体过程如下。

（1）路由器 B 从隧道接口收到 IP 报文，检查目的地址。

（2）因为路由器 B 是隧道的末端路由器，所以路由器 B 去掉 IP 报文的头部信息，交给 GRE 协议模块处理。

（3）GRE 协议模块完成相应的处理（如密码验证、报文的序列号检查等）后，去掉 GRE 头部信息，将封装之前的净载荷交给 IPX/SPX 网络 B。

（4）IPX/SPX 协议模块对该报文进行后续的转发处理。

2. GRE 的安全性

为了提高 GRE 隧道的安全性，GRE 支持对隧道端口的认证和对隧道封装的报文进行端到端校验功能。在 RFC 1701 中规定，如果 GRE 报文头部信息中的 Key 标识设置为 1，则收发双方将进行通道识别关键字（或密码）的验证，只有隧道两端设置的识别关键字完全（或密码）一致时才能通过验证，否则将报文丢弃。如果 GRE 报文头部信息中 Checksum 标

识位置为1,则需要对隧道中传输的GRE报文进行校验。发送方将对图9-13中的GRE头部及封装后的数据包计算校验和,并将包含校验和的报文发送给隧道对端。接收方对接收到的报文计算校验和,并与报文中的校验和比较,如果一致则对报文进一步处理,否则丢弃。

由于GRE提供的安全特性较弱,所以可以将IPSec安全体系应用到GRE中,以提高GRE的安全性。

9.4.2 IPSec

IPSec(IP Security)是IETF的IPSec工作组于1998年制订的一组基于密码学的开放网络安全协议。IPSec工作在网络层,为网络层及以上层提供访问控制、无连接的完整性、数据来源认证、防重放保护、保密性和自动密钥管理等安全服务。IPSec是一套由多个子协议组成的安全体系。

1. IPSec体系结构

IPSec主要由AH(Authentication Header,认证头部)协议、ESP(Encapsulating Security Payload,封装安全载荷)协议和负责密钥管理的IKE(Internet Key Exchange,Internet密钥交换)协议组成。IPSec通过AH协议和ESP协议来对网络层或上层协议进行保护,通过IKE协议进行密钥交换。各协议之间的关系如图9-15所示。

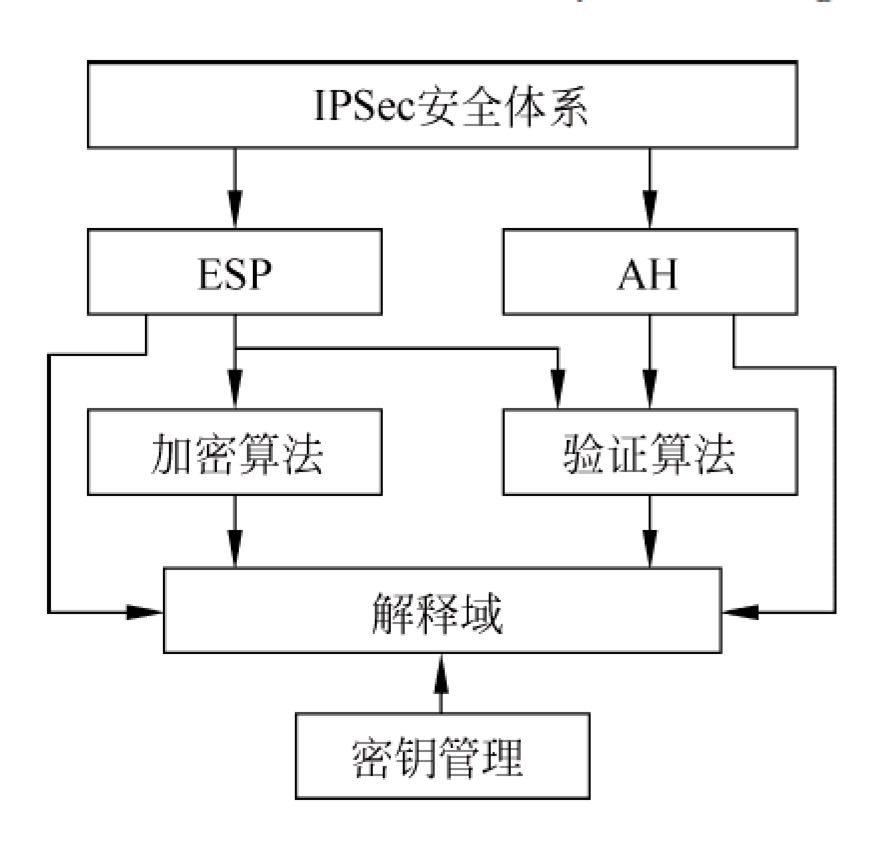


图9-15 IPSec安全体系结构示意图

(1) AH。为IP数据报提供无连接的数据完整性和数据源身份认证,同时具有防重放(replay)攻击的能力。可通过消息认证(如MD5)产生的校验值来保证数据完整性;通过在待认证的数据中加入一个共享密钥来实现数据源的身份信证;通过AH头部的序列号来防止重放攻击。AH的详细内容可参看RFC 2402文档。

(2) ESP。为IP数据报提供数据的保密性(通过"加密算法"来实现)、无连接的数据完整性和数据源身份认证及防重放攻击保护。与AH相比,数据保密性是ESP的新增功能。ESP中的数据源身份认证、数据完整性校验和防重放攻击保护的实现与AH相同。ESP的详细内容可参看RFC 2406文档。

需要说明的是,AH和ESP既可以单独使用,也可以配合使用。由于ESP提供了对数据的保密性,所以在目前的实际应用中多使用ESP,而很少使用AH。

(3) 解释域(DOI)。解释域将所有的IPSec协议捆绑在一起,为IPSec的安全性提供综合服务。例如,当系统中同时使用了ESP和AH时,解释域将两者的安全性进行集成。

(4) IKE。IKE协议是密钥管理的一个重要组成部分,它在通信系统之间建立安全关联,提供密钥确定、密钥管理的机制,是一个产生和交换密钥并协调IPSec参数的框架。IKE将密钥协商的结果保留在SA(安全关联)中,供AH和ESP通信时使用。IKE的详细内容可参看RFC 2409文档。

2. IPSec的工作模式

IPSec协议可以在两种模式下运行:传输模式和隧道模式。其中,传输模式使用原来的

IP 头部，把 AH 或 ESP 头部插入到 IP 头部与 TCP 头部之间，为上层协议提供安全保护。传输模式保护的是 IP 数据报中的有效载荷(上层的 TCP 报文段或 UDP 数据报)。传输模式的 IPSec 组成结构如图 9-16(a)所示。

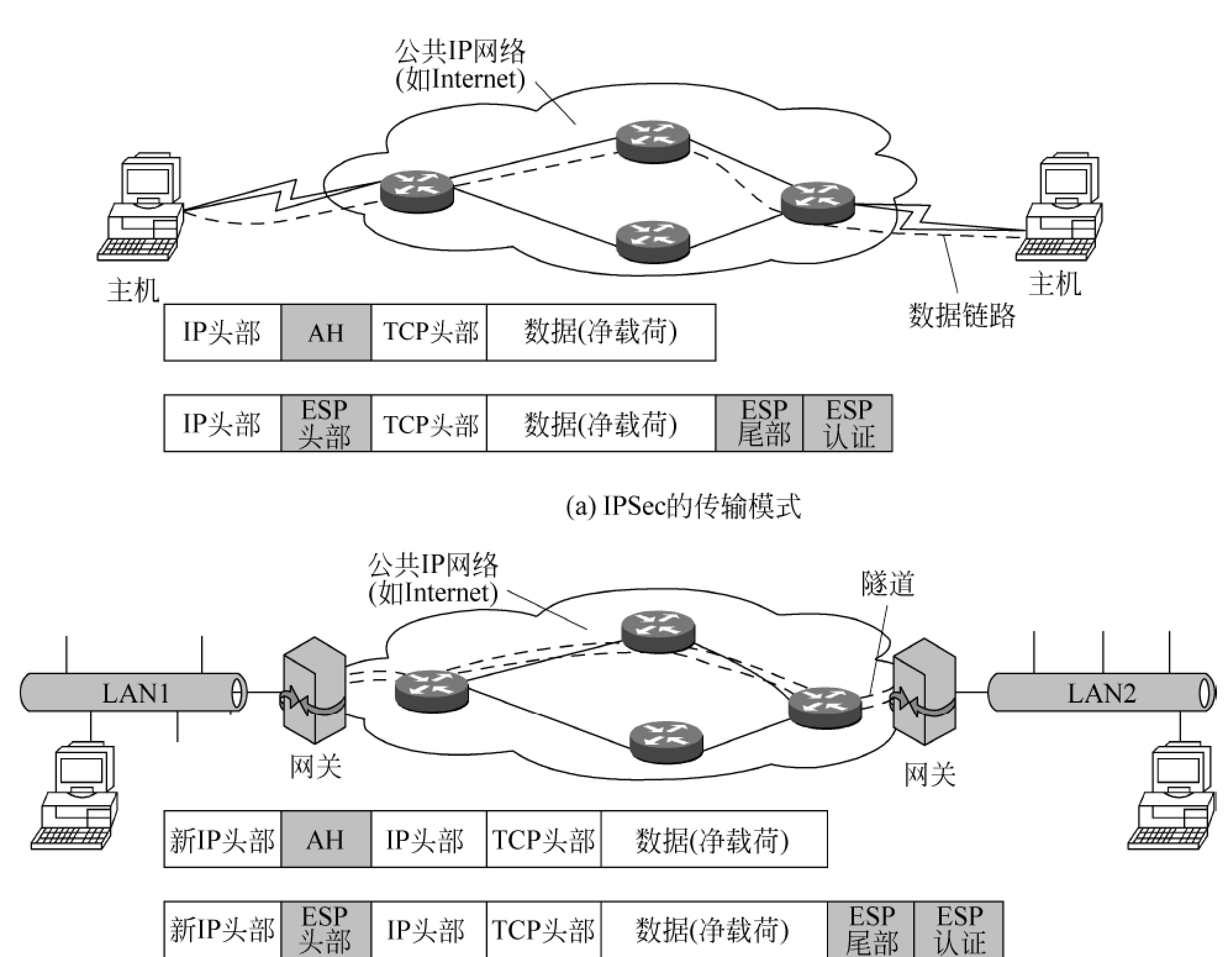


图 9-16　IPSec 的工作模式

隧道模式首先为原始 IP 数据报增加 AH 或 ESP 头部，然后再在外部添加一个新 IP 头部。原来的 IP 数据报通过这个隧道从 IP 网络的一端传递到另一端，途中所经过的路由器只检查最外面的 IP 头部(新 IP 头部)，而不检查原来的 IP 数据。由于增加了一个新 IP 头部，因此新 IP 数据报的目的地址可能与原来的不一致。隧道模式的 IPSec 组成结构如图 9-16(b)所示。

IPSec 的传输模式实现了主机之间端到端的安全保障，AH 和 ESP 保护的是用户数据(净载荷)。在通常情况下，传输模式只用于两台主机之间的安全通信。隧道模式为整个 IP 数据报提供了安全保护。隧道模式通常用在隧道的其中一端或两端是安全网关(防火墙、路由器等)的网络环境中。使用隧道模式后，安全网关后面的主机可以使用内部私有 IP 地址进行通信，而且在内部通信中不需要使用 IPSec。

传输模式下的 IPSec 数据包未对原始 IP 头部提供加密和认证，因而存在利用 IP 头部信息进行网络攻击的隐患。传输模式的优点是对原始数据包的长度增加很少，因此占用系统的开销也较小。在隧道模式下，由于原始数据包成了新数据包的净载荷，所以安全性较高，但对系统的开销较大。

3. AH

如图 9-15 所示，在 IPSec 安全体系中，AH 通过验证算法为 IP 数据报提供了数据完整性和数据源身份认证功能，同时还提供了防重放攻击能力（可选），但 AH 协议不提供数据加密功能。

（1）数据完整性。是指保证数据在存储或传输过程中，其内容未被有意或无意改变。

（2）数据源身份认证。是指对数据的来源进行真实性认证，认证依据主要有源主机标识、用户账户和网络特性（IP 地址、接口的物理地址等）。

（3）重放攻击。是指攻击者通过重放消息或消息片段达到对目标主机进行欺骗的攻击行为，其主要用于破坏认证的正确性。

AH 头部位于 IP 头部和传输层协议头部之间。“而在隧道模式中，AH 位于新 IP 头部与原 IP 数据报之间”，如图 9-17 所示。AH 可以单独使用，也可以与 ESP 协议结合使用。

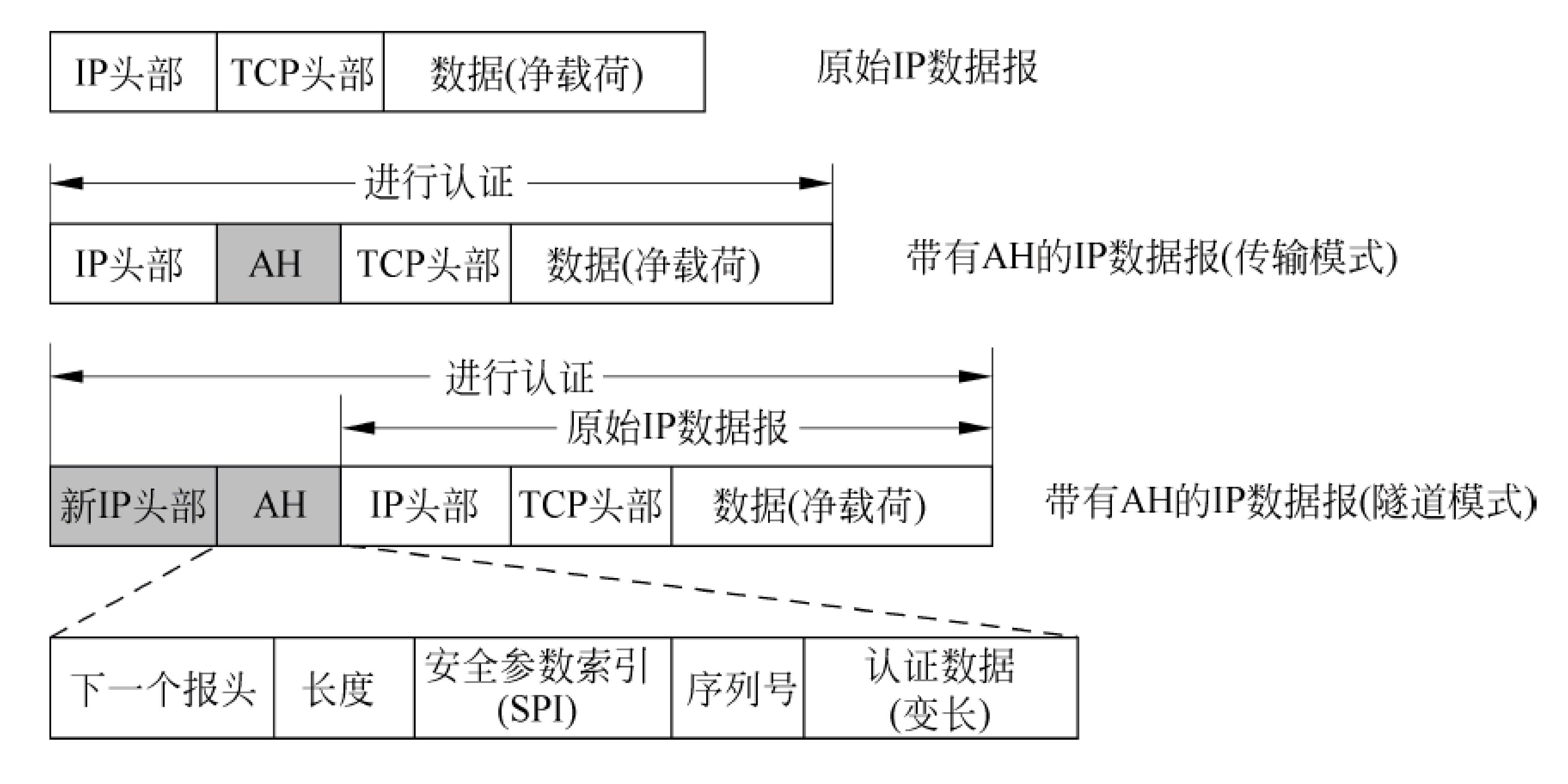


图 9-17　AH 的认证方式及协议组成

- 下一个报头（Next Header）。用于识别在 AH 后面的一个 IP 数据报的类型。在传输模式下，将是原始 IP 数据报的类型，如 TCP 或 UDP；在隧道模式下，如果采用 IPv4 封装时这一字段值设置为 4，如果是 IPv6 封装时这一字段值设置为 41。
- 长度（Length）。AH 头部信息的长度。由于在 AH 头部信息中还设置了“保留”字段（图 9-17 未标出），在不同应用中 AH 头部的长度是不确定的，所以对于某一个具体应用来说需要标明整个 AH 头部的长度值。
- 安全参数索引（Security Parameters Index，SPI）。在 AH 头部中，SPI 字段的长度为 32 位。SPI 的值可以任意设置，它与 IP 头部（如果是隧道模式，则为“新 IP 头部”）中的目的 IP 地址一起用于识别数据报的安全关联。其中，当 SPI 为 0，被保留用来表明“没有安全关联存在”。
- 序列号（Sequence Number）。序列号字段的长度为 32 位，它是一个单向递增的计数器，不允许重复，用于唯一地标识每一个发送数据包，为安全关联提供防重放攻击的保护。接收端通过校验序列号，确定使用某一序列号的数据包是否已经被接收过，如果已接收过，则拒收该数据包，避免了重放攻击的发生。
- 认证数据（Authentication Data）。认证数据字段是一个可变长度的字段，但该字段中包含一个非常重要的项，即完整性检查和（ICV），它是一个 Hash 函数值。接收端

在接收到数据包后，首先执行相同的 Hash 运算，将运算值再与发送端所计算的 ICV 值进行比较，如果两者相同，表示数据完整。如果数据在传输过程中被篡改，则两个计算结果将不一致。

4. ESP

ESP 为 IP 数据报提供数据的保密性（通过加密实现）、无连接的数据完整性、数据源身份认证及防重放攻击的功能。其中，ESP 安全协议的特点如下。

（1）ESP 服务依据建立的安全关联是可选的。

（2）数据完整性检查和数据源身份认证一起进行。

（3）仅当与数据完整性检查和数据源身份认证一起使用时，防重放攻击保护才是可选的。

（4）防重放攻击保护只能由接收方选择使用。

（5）ESP 的加密服务是可选的，但当启用了加密功能后，也就选择了数据完整性检查和数据源身份认证。因为仅使用加密功能对 IPSec 系统来说是不安全的。

（6）ESP 可以单独使用，也可以和 AH 结合使用。一般 ESP 不对整个 IP 数据报加密，而是只加密 IP 数据报的有效载荷部分，不包括 IP 头部。但在端对端的隧道通信中，ESP 需要对整个原始数据报进行加密。

ESP 的安全体系和协议组成如图 9-18 所示。其中 ESP 头部包括安全参数和序列号两个字段，其功能描述与 AH 相同。ESP 尾部包括如下内容。

- 扩展位（Padding）。其值在 0～255B（字节）之间。主要是在进行数据加密处理的过程中，为了使加密数据的长度符合某一加密算法的要求（如是 512 的整数倍），或在加密时隐藏用户数据的真实长度，就使用扩展位来填充。
- 扩展位长度（Padding Length）。它是 ESP 尾部的必选字段，表示扩展位的长度值。如果该字段值为 0，表示没有扩展（没有使用填充）。
- 下一个报头。用于识别在 AH 后面的一个 IP 数据报的类型，具体含义与 AH 协议中的下一个报头的定义相同。

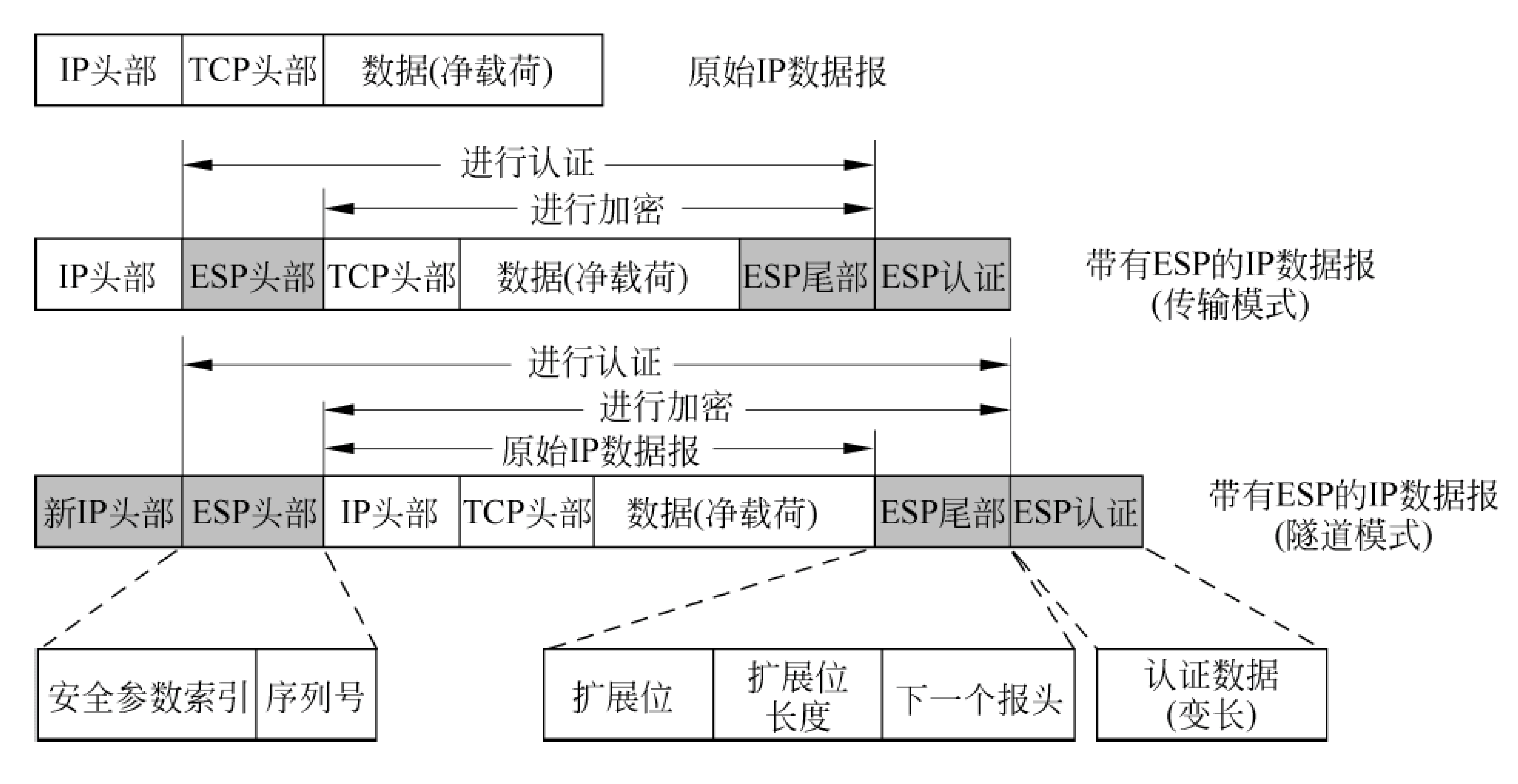


图 9-18　ESP 的安全体系和协议组成

ESP 认证部分仅包含一个认证数据(Authentication Data)字段,只有在安全关联中启用了认证功能时,才会有此字段。其功能与 AH 中的数据认证字段的定义相同,但要认证的字段包括 ESP 头部、原始 IP 数据报和 ESP 尾部。

5. IKE

IKE(Internet Key Exchange,Internet 密钥交换协议)是 IPSec 规定的一种用来动态创建安全关联的密钥协商协议。在 IPSec 系统中,IKE 对 SA 进行协商,并对安全关联数据库(SAD)进行维护。IKE 是 IETF 提出的一种混合型协议,按照其框架设计,采用三个 RFC 文档来定义 IKE 协议。

(1) ISAKMP(Internet Security Association and Key Management Protocol)。定义了一个密钥交换的基本框架,包括报文格式、报文如何解析和密钥协商过程等。

(2) IPSec DOI(IPSec Domain of Interpretation)。它是对 ISAKMP 应用于 IPSec 解释域的描述,规定了 ISAKMP 和 IKE 究竟要协商什么。

(3) IKE。是符合 ISAKMP 的一个密钥交换协议。IKE 是在 ISAKMP 的框架下定义的,它的某些细节又在 IPSec DOI 中进行描述。同时,IKE 还采用了 Oakley(Oakley 密钥管理协议)的部分交换模式,以及 SKEME(Secure Key Exchange Mechanism,安全密钥交换机制)协议的共享和密钥更新技术。

① IKE 协商 SA 的两个阶段。第一阶段的主要目的在于验证对方的身份,从而得到 ISAKMP SA,为第二阶段建立一个安全信道;第二阶段是在第一阶段协商的基础上利用找到的 IPSec 安全策略库中的相应策略进行协商,建立实际使用的 IPSec SA。一个 ISAKMP SA 可用来建立多个 IPSec SA。

② 模式。IKE 协议规定了主模式、野蛮模式、快速模式和新群模式 4 种模式。其中第一阶段只能采用主模式或野蛮模式中的一种,两种模式的区别是:主模式包括 6 条消息,交换过程提供身份认证;野蛮模式只包括 3 条消息,如果不使用公钥验证方法,交换过程不提供身份认证功能。第二阶段只能采用快速模式。新群模式既不属于第一阶段,也不属于第二阶段,它跟在第一阶段之后,利用第一阶段的协商结果来协商新的群参数。

③ 验证方法。IKE 协议指定第一阶段可以使用下列方式进行验证。

- 预共享密钥。通信双方通过某种安全途径获取交换双方唯一共享的密钥,通过 Hash 运算来完成认证。
- 数字签名。通信双方利用自己的私钥对特定的信息进行签名,对方利用获得的公钥进行解密处理,以确定对方的身份,完成认证过程。
- 公钥加密。通信双方利用对方的公钥来加密特定的信息,同时根据对方返回的结果以确定对方的身份。在 IKE 协议中可采用两种加密方法:一种是一次公钥加密,一次私钥解密;另一种是两次公钥加密,两次私钥解密。

9.5 VPN 实现技术

本章前面重点介绍了第二层和第三层隧道协议的实现原理及应用特点,隧道协议是 VPN 的基础。对于用户来说,可以利用公共网络基础设施,通过 VPN 实现多个内部网络之间的远程互联;对于电信运营商来说,VPN 已成为目前最具潜力的业务之一。所以,不管

是企业用户还是电信运营商，VPN 都蕴含着极大的商机，已经成为提供新一代电信业务的基石。近年来，VPN 在网络互联和用户远程接入中得到了广泛应用，本节介绍的 MPLS VPN 和 SSL VPN 则是目前应用领域的主流技术。

9.5.1 MPLS VPN

IP 技术和 ATM 技术是现代计算机通信系统中的两大技术支柱。然而，随着各类应用需求的不断出现，人们希望以 Internet 为主的 IP 网络不仅仅能够提供传统的电子邮件、上网浏览等需求，而且还能够提供在线视频、交互式应用等宽带、实时性业务。ATM 曾经被普遍认为是能够提供多种业务的快速交换技术，但是由于 IP 技术已经成为应用中既成事实的网络标准，致使现在的 ATM 网络主要用来承载 IP 数据流。在此情况下，人们希望 IP 数据流也能提供类似于 ATM 的多种类型的服务，而 ATM 在应用领域也急需要得到功能的扩展。MPLS(Multiprotocol Label Switch，多协议标签交换)便是其中一种被业界看好的解决方案。在现有的 MPLS 应用中，MPLS VPN 的技术最为成熟、应用最为广泛。2002 年，美国 *Telecommunications* 杂志将 MPLS VPN 技术评为十大热门技术之一。

1. MPLS 的概念和组成

MPLS 是一个可以在多种第二层网络(如 ATM、帧中继、以太网和 PPP 等)上进行标签交换的网络技术。这一技术结合了第二层交换和第三层路由的特点，将第二层的基础设施和第三层的路由有机地结合起来。第三层的路由在网络的边缘实施，而在 MPLS 的网络核心采用第二层交换。

MPLS 是一种特殊的转发机制，它为进入网络中的 IP 数据包分配标签，并通过对标签的交换来实现 IP 数据包的转发。标签位于 IP 数据包的头部，在 MPLS 内部通过标签来替代原有的 IP 地址来寻址。在 MPLS 网络内部，带有标签的数据包在到达某一节点(如路由器)时，节点通过交换数据包的标签(而不是 IP 地址)来实现转发。当数据包要离开 MPLS 网络时，数据包被去掉入口处添加的标签，继续按照 IP 包的路由方式到达目的网络。

如图 9-19 所示，MPLS 网络主要由核心部分的标签交换路由器(Label Switching Router，LSR)、边缘部分的标签边缘路由器(Label Edge Router，LER)和在节点之间建立和维护路径的标签交换路径(Label Distribution Path，LSP)组成。

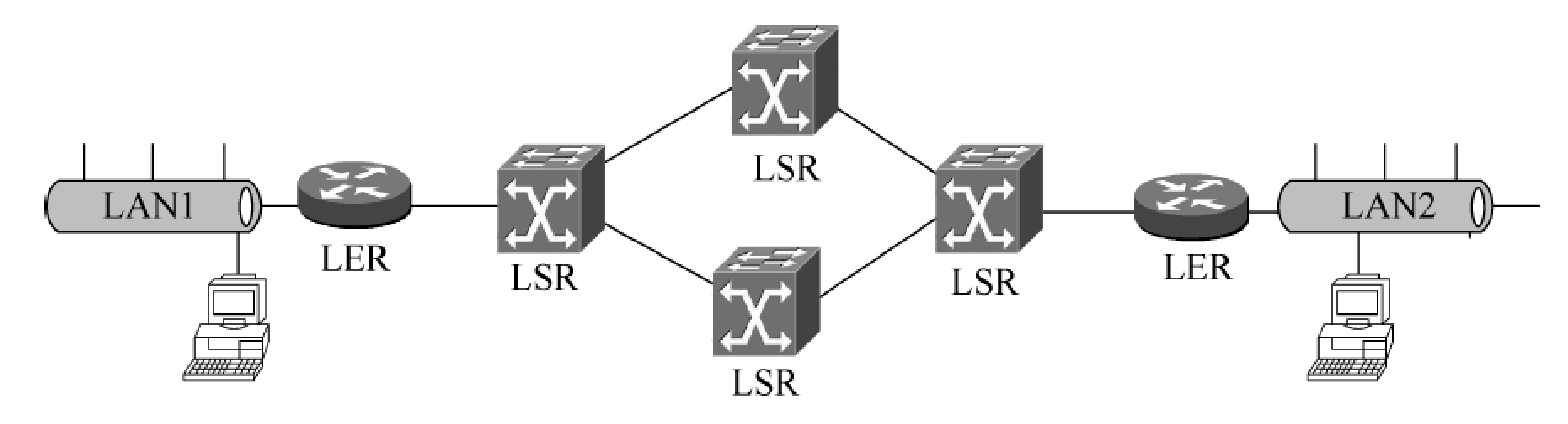


图 9-19　MPLS 网络的组成

(1) LSR。它的作用可以看作是 ATM 交换机与传统路由器的结合，提供数据包的高速交换功能。LSR 位于 MPLS 网络的中心，主要完成运行 MPLS 控制协议(如 LDP)和第三层的路由协议。同时，负责与其他的 LSR 交换路由信息，建立完善的路由表。

(2) LER。作用是分析 IP 数据包的头部信息，在一端负责 IP 数据包进入 MPLS 网络，在另一端负责 IP 数据包离开 MPLS 网络。同时，在 LER 处可以实现对业务的分类、分发

标签及去掉标签(在另一端),而且还可以实现策略管理和流量工程控制等功能。其中流量工程控制是 MPLS 除 VPN 之外的另一项重要应用。传统 IP 网络一旦为某一个 IP 数据包选择了一条路径,IP 数据包就会沿着这条路径传输,而不管这一条路径是否出现阻塞或还有更好的路径可供选择。MPLS 可以控制 IP 数据包在网络中的传输路径,动态地选择目前的最佳路径进行 IP 数据包的传输。

(3) LSP。在 MPLS 节点之间的路径称为标签交换路径。当 MPLS 在分配标签的过程中便建立了一条 LSP。LSP 可以是动态的,由路由信息自动生成;也可以是静态的,由人工进行设置。LSP 可以看作是一条贯穿网络的单向隧道,所以当两个节点之间要进行全双工通信时需要两条 LSP。

另外,为了控制 LSR 之间交换标签和绑定信息,以及协调 LSR 之间的工作,MPLS 还提供了标签分配协议(Label Distribution Protocol,LDP)。LDP 是 MPLS 的核心部分,LDP 将某一个 LSR 生成的标签及其隐含在标签中的信息传送给相邻的 LSR,从而在相邻 LSR 之间建立一条信息传输的通道。正是 LDP 具有的标签分发功能,所以能够使 LSR 之间在标签的分发、使用和维护中达到一致性,进而建立一条从一端的 LER 到另一端的 LER 的完整 LSP。

2. MPLS 的工作过程

如图 9-20 所示,MPLS 的工作过程如下。

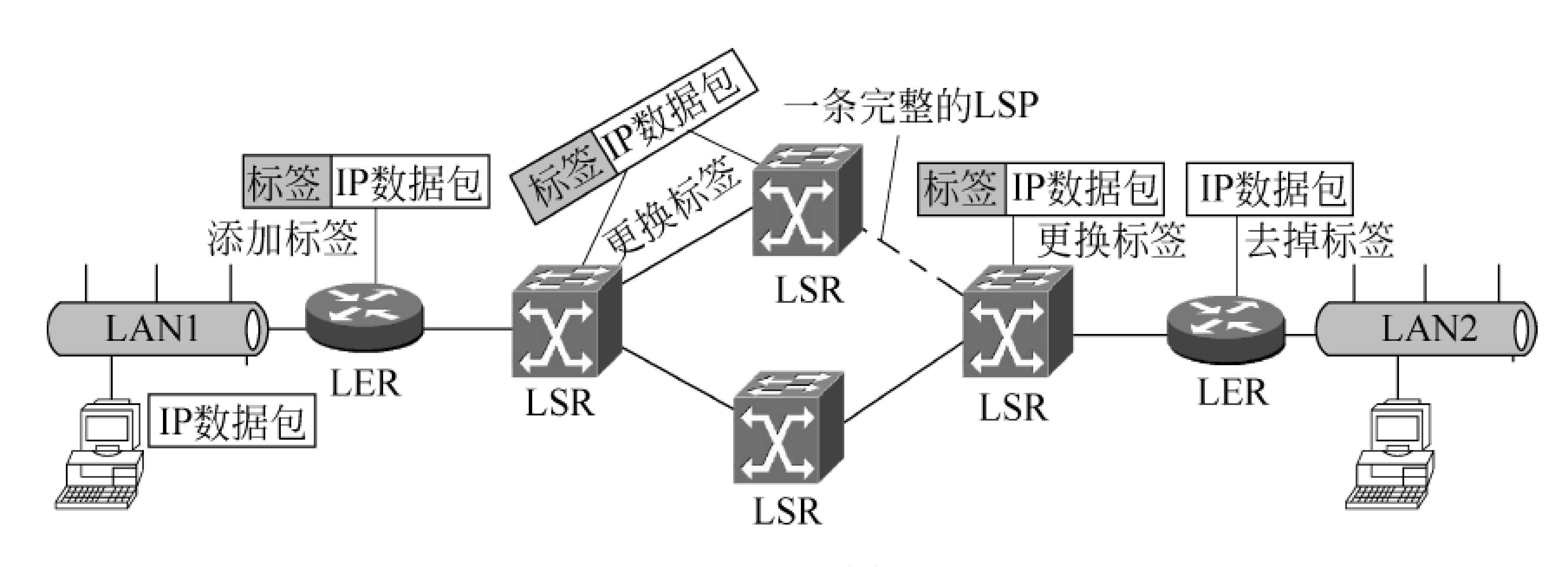


图 9-20 MPLS 中 IP 数据包的转发过程

(1) 由标签分配协议和传统路由协议(如 OSPF、RIP 等)共同在各个 LSR 中为需要使用 MPLS 服务的转发等价类(FEC)建立标签交换转发表和路由表。

其中,转发等价类(Forwarding Equivalence Class,FEC)是指一组具有相同的转发特征的 IP 数据包,当 LSR 接收到这一组 IP 数据包时将会按照相同的方式来处理每一个 IP 数据包,如从同一个接口转发到相同的下一个节点,并具有相同的服务类别和服务优先级。FEC 与标签是一一对应的,标签用来绑定 FEC,即用标签来表示属于一个从上游 LSR 流向下游 LSR 的特定 FEC 的分组。标签的结构如图 9-21 所示,其中各部分的内容如下。

- Label。该字段为标签字段,占用 20 位的长度,用于存放与相邻节点(LER 和 LSR)的 LSP 等信息相关的标识符。

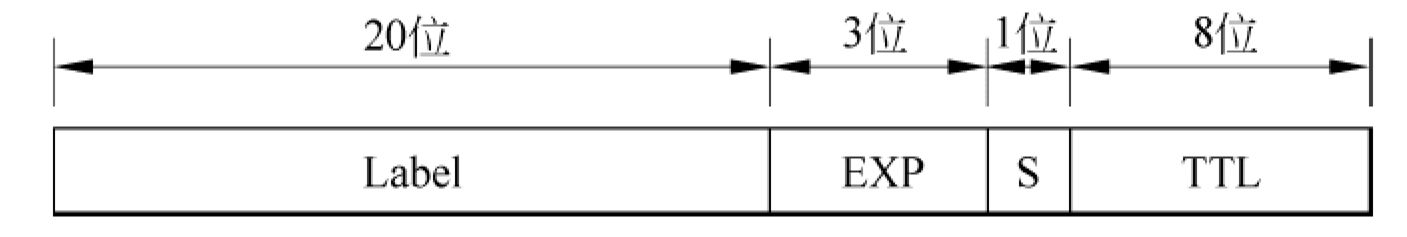


图 9-21 MPLS 中标签的结构

- EXP。该字段为实验字段，占用3位的长度，用于标记该MPLS中IP数据包的优先级，实现不同的服务质量。
- S。该字段占用1位的长度，为堆栈(Stack)字段。当S的值为1时，表示在该标签内部还有标签，否则为0。
- TTL。该字段表示生存周期，占用8位的长度。是IP数据包在网络中经过的最大路由节点数。

值得注意的是，LDP信令及标签绑定信息只在MPLS相邻节点间传递。LSR之间或LSR与LER之间依然需要运行标准的路由协议(如OSPF、RIP等)，并由此获得网络拓扑信息。通过这些信息，LSR可以明确选取IP数据包的下一跳并可最终建立特定的LSP。

(2) 在MPLS网络的入口处为IP数据包添加标签。LER接受IP数据包，完成第三层的功能(如带宽管理、QoS等)，判定IP数据包所属的FEC，根据IP数据包中的目的地址或有关服务质量等信息映射规则，将IP数据包的头部信息和固定长度的标签对应起来。这样就给IP数据包加上了标签，形成了MPLS标签分组并通过标签中标明的接口转发出去。

(3) 在LSP上进行标签交换。在IP数据包以后的网络转发过程中(即在MPLS域内)，LSR只是根据IP数据包所携带的标签来进行标签交换和数据转发，不再进行任何第三层(如IP路由寻址)处理。在每一个节点上，LSR首先去掉由前一个节点添加的标签，然后将一个新的标签添加到该IP数据包的头部，并告诉下一跳(下一个节点)如何转发它。

(4) 在出口处为IP数据包去掉标签。在MPLS的出口LER上，将IP数据包中的标签去掉，然后继续进行转发。

3. MPLS VPN的概念和组成

在学习了MPLS的相关知识后，下面学习MPLS VPN的有关内容。MPLS VPN是利用MPLS中的LSP作为实现VPN的隧道，用标签和VPN ID将特定VPN的数据包进行唯一识别。在无连接的网络上建立的MPLS VPN，所建立的隧道是由路由信息的交互而得的一条虚拟隧道(即LSP)。

与本章前面介绍的基于第二层和第三层隧道协议的VPN相比较，MPLS VPN可以充分利用MPLS技术的一些优势，为用户提供更安全、可靠的隧道连接服务。例如，MPLS的流量工程控制、服务质量等。对于电信运营商来说，只需要在网络边缘设备(LER)上启用MPLS服务，对于大量的中心设备(LSR)不需要进行配置，就可以为用户提供MPLS VPN等服务业务。根据电信运营商边界设备是否参与用户端数据的路由，运营商在建立MPLS VPN时有两种选择：第二层的解决方案，通常称为第二层MPLS VPN；第三层解决方案，通常称为第三层MPLS VPN。在实际应用中，MPLS VPN主要用于远距离连接两个独立的内部网络，这些内部网络一般都提供有边界路由器，所以多使用第三层MPLS VPN来实现。下面将以第三层MPLS VPN为例进行介绍。如图9-22所示，一个MPLS VPN系统主要由以下几个部分组成。

(1) 用户边缘(Custom Edge，CE)设备。CE设备属于用户端设备，一般由单位用户提供，并连接到电信运营商的一个或多个PE路由器。通常情况下，CE设备是一台IP路由器或三层交换机，它与直连的PE路由器之间通过静态路由或动态路由(如RIP、OSPF等)建立联系。之后，CE将站点的本地路由信息广播给PE路由器，并从直连的PE路由器学习到远端的路由信息。

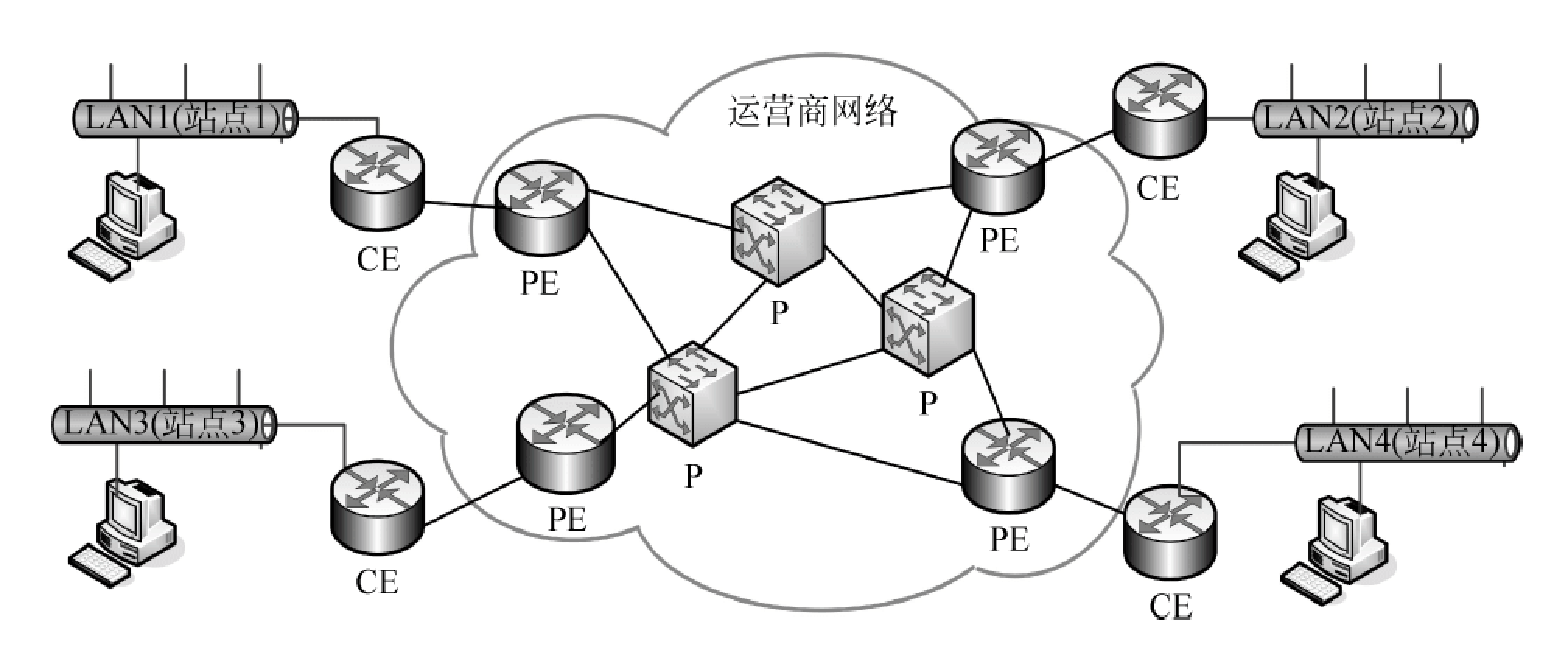


图 9-22　MPLS VPN 的组成

（2）提供商边缘（Provider Edge，PE）设备。PE 路由器为其直连的站点维持一个虚拟路由转发表（VRF），每个用户链接被映射到一个特定的 VRF。需要说明的是，一般在一个 PE 路由器上同时会提供多个网络接口，而多个接口可以与同一个 VRF 建立联系。PE 路由器具有维护多个转发表的能力，以便每个 VPN 的路由信息之间相互隔离。PE 路由器相当于 MPLS 中的 LER。

（3）提供商（Provider，P）设备。P 路由器是电信运营商网络中不连接任何 CE 设备的路由器。由于数据在 MPLS 主干网络中转发时使用第二层的标签堆栈，所以 P 路由器只需要维护到达 PE 路由器的路由，并不需要为每个用户站点维护特定的 VPN 路由信息。P 路由器相当于 MPLS 中的 LSR。

（4）用户站点（site）。是在一个限定的地理范围内的用户子网，一般为单位用户的内部局域网。

4．MPLS VPN 的数据转发过程

在 MPLS VPN 中，通过以下 4 个步骤完成数据包的转发。

（1）当 CE 设备将一个 VPN 数据包转发给与之直连的 PE 路由器后，PE 路由器查找该 VPN 对应的 VRF，并从 VRF 中得到一个 VPN 标签和下一跳（下一节点）出口 PE 路由器的地址。其中，VPN 标签作为内层标签首先添加在 VPN 数据包上，接着将在全局路由表中查到的下一跳出口 PE 路由器的地址作为外层标签再添加到数据包上。于是，VPN 数据包被封装了内、外两层标签。

（2）主干网的 P 路由器根据外层标签转发 IP 数据包。其实，P 路由器并不知道它是一个经过 VPN 封装的数据包，而把它当作一个普通的 IP 分组来传输。当该 VPN 数据包到达最后一个 P 路由器时，数据包的外层标签将被去掉，只剩下带有内层标签的 VPN 数据包，接着 VPN 数据包被发往出口 PE 路由器。

（3）出口 PE 路由器根据内层标签查找到相应的出口后，将 VPN 数据包上的内层标签去掉，然后将不含标签的 VPN 数据包转发给指定的 CE 设备。

（4）CE 设备根据自己的路由表将封装前的数据包转发到正确的目的地。

综上所述，MPLS VPN 的优势在于可以通过相同的网络结构来支持多种 VPN，并不需要为每一个用户分别建立单独的通道。同时，MPLS VPN 将基于 IP 网络的 VPN 功能内置于网络本身，无需进行复杂的配置和管理。

9.5.2 SSL VPN

本章前面介绍的 MPLS VPN 是由电信运营商为企业用户提供的一种实现内部网络之间远程互联的业务，而本节将要介绍的 SSL VPN 主要供企业移动用户访问内部网络资源时使用。

1. SSL VPN 的功能

SSL VPN 是一种借助 SSL 协议实现安全 VPN 通信的远程访问解决方案。远程用户通过 SSL VPN 能够访问企业内部的资源，这些资源包括 Web 服务、文件服务(包括 FTP 服务、Windows 网上邻居服务)、可转换为 Web 方式的应用(如 Webmail)及基于 C/S 的各类应用等。SSL VPN 属于应用层的 VPN 技术，VPN 客户端与服务器之间通过 https 安全协议来建立连接和传输数据。

SSL VPN 的核心是 SSL 协议。SSL 协议是基于 Web 应用的安全协议，它指定了在应用层协议(如 HTTP、Telnet 和 FTP 等)和 TCP/IP 协议之间进行数据交换的安全机制，为 TCP/IP 连接提供数据加密、服务器认证及可选的客户机认证等功能，有关 SSL 协议的详细内容已在本书第 4 章进行了专门介绍。

目前 SSL VPN 的应用模式基本上分为三种：Web 浏览器模式、SSL VPN 客户端模式和 LAN 至 LAN 模式。其中，由于 Web 浏览器模式不需要安装客户端软件，只需通过标准的 Web 浏览器(如 Windows 操作系统的 IE 等)连接 Internet，即可以通过私有隧道访问到企业内部的网络资源。这样无论是从软件购买成本，还是从系统的维护、管理成本上都具有一定的优势，所以 Web 浏览器模式的应用最为广泛。不过，需要说明的是，SSL VPN 并非"无需安装客户端软件"，而是可以不单独安装客户端软件。根据用户需要，现在大部分 SSL VPN 系统既可以使用专门的 SSL VPN 客户端软件，也可以直接使用标准的 Web 浏览器。当使用标签的 Web 浏览器时，一般需要安装专门的 Web 浏览器控件(插件)。本节主要以 Web 浏览器模式为主介绍 SSL VPN 的实现原理和主要应用。

2. 基于 Web 浏览器模式的 SSL VPN

基于 Web 浏览器模式的 SSL VPN 在技术上将 Web 浏览器软件、SSL 协议及 VPN 技术进行了有机结合，在使用方式上可以利用标准的 Web 浏览器，并通过遍及全球的 Internet 实现与内部网络之间的安全通信，已成为目前应用最为广泛的 VPN 技术。

如图 9-23 所示，SSL VPN 客户端使用标准 Web 浏览器通过 SSL VPN 服务器(也称为 SSL VPN 网关)访问单位内部网络中的资源。在这里，SSL VPN 服务器扮演的角色相当于一个用于数据中转的代理服务器，所有 Web 浏览器对内部网络中以 Web 方式提供的资源的访问都经过 SSL VPN 服务器的认证。内部网络中的服务器(如 Web、FTP 等)发往 Web 浏览器的数据经过 SSL VPN 服务器加密后送到 Web 浏览器，从而在 Web 浏览器和 SSL VPN 服务器之间由 SSL 协议构建了一条安全通道。

在以上通信过程中，需要注意以下几点。

(1) SSL VPN 系统是由 SSL、HTTPS 和 COSKS 这三个协议相互协作来实现的。其中，SSL 协议作为一个安全协议，为 VPN 系统提供安全通道；HTTPS 协议使用 SSL 协议保护 HTTP 应用的安全；COCKS 协议实现代理功能，负责转发数据。SSL VPN 服务器同时使用了这三个协议，而 SSL VPN 客户端对这三个协议的使用有所差别，Web 浏览器只使

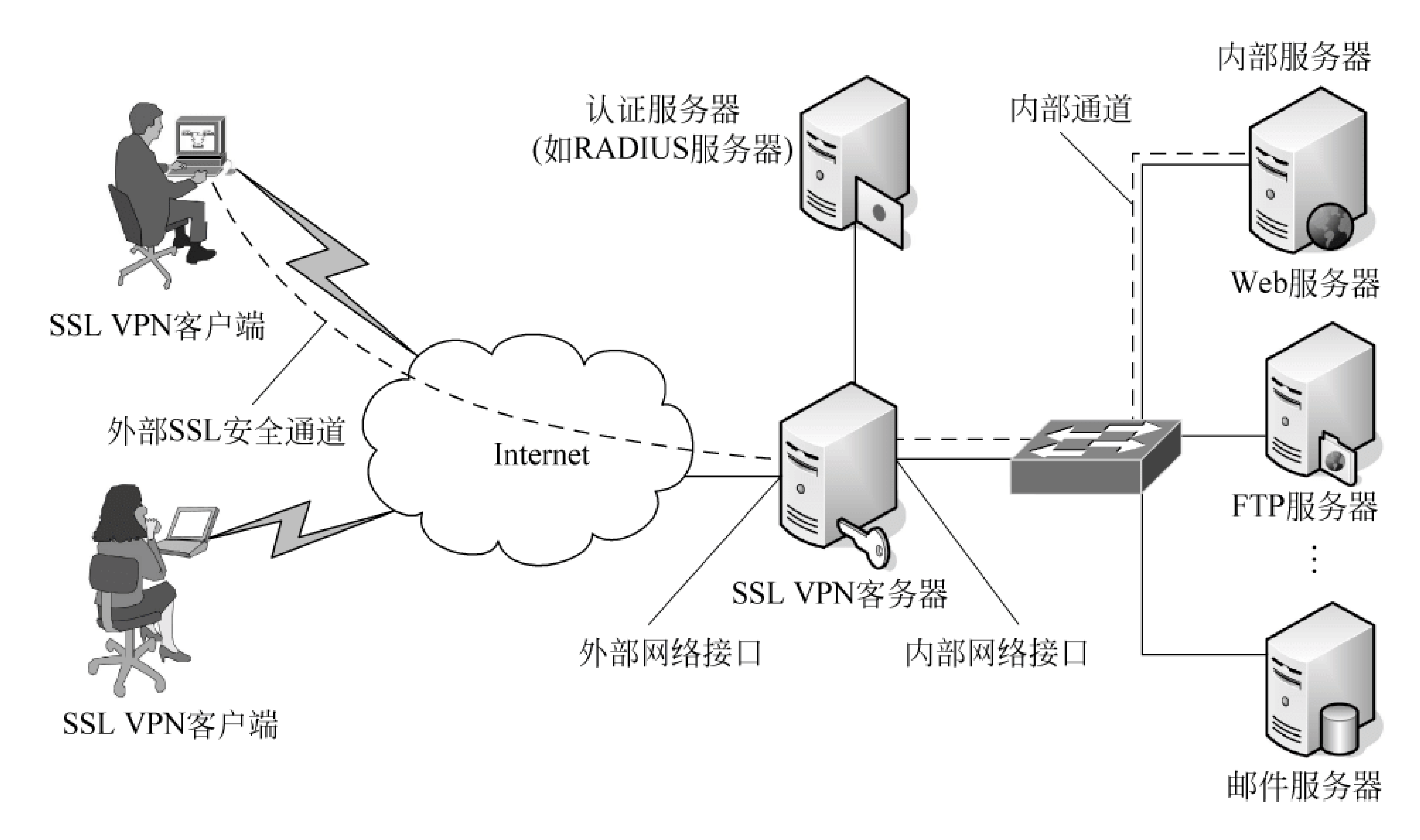


图 9-23 基于 Web 浏览器模式的 SSL VPN 的工作过程

用 HTTPS 和 SSL 协议，而 SSL VPN 客户端程序则使用 SOCKS 和 SSL 协议。

（2）SSL VPN 客户端与 SSL VPN 服务器之间通信时使用的是 HTTPS 协议。由于 HTTPS 协议是建立在 SSL 协议之上的 HTTP 协议，所以在 SSL VPN 客户端与 SSL VPN 服务器之间进行通信时，首先要进行 SSL 握手，握手过程结束后再发送 HTTP 数据包。

（3）SSL VPN 服务器与单位内部网络中的服务器之间的通信使用的是 HTTP 协议。SSL VPN 客户端对发送的数据首先进行加密处理，然后通过 HTTPS 协议发送给 SSL VPN 服务器。当 SSL VPN 服务器接收到 SSL VPN 客户端的该数据后，解密该数据，得到明文的 HTTP 数据包。然后，SSL VPN 服务器将 HTTP 数据包利用内部的数据通信传输给要访问的资源服务器。从内部资源服务器到 SSL VPN 客户端的数据传输过程正好相反。

（4）HTTP 代理。SSL VPN 服务器提供了 HTTP 代理功能。HTTP 代理用于将客户端的请求转发给内部服务器，同时将内部服务器的响应转发给客户端。在 SSL VPN 系统中，SSL VPN 服务器相当于一台代理服务器，它将客户端与服务器之间的通信进行了隔离，隐藏了内部网络的信息。不过，HTTP 代理是基于 TCP 协议的，UDP 数据报无法通过 HTTP 代理。如果客户端需要通过 HTTP 代理来访问 UDP 服务，客户端就需要将 UDP 数据报转换为 TCP 报文段，再发送给 HTTP 代理，而 HTTP 代理在接收到 TCP 报文段后将它再还原为 UDP 数据报，并转发给目的服务器。

（5）可 Web 化应用。凡是可以通过应用转换，隐藏其真实应用协议和端口，以 Web 页面方式提供给用户的应用协议，称为可 Web 化应用。例如，当使用邮件客户端软件（如 Foxmail、Outlook 等）进行邮件收发操作时，邮件服务器需要同时开放 POP3 协议的 110 号端口和 SMTP 协议的 25 号端口。但是，在支持 Webmail 方式的邮件系统中，用户可以通过访问 Web 页面来收发邮件，邮件系统向用户隐藏了真正的邮件服务器所提供的端口。

(6) 客户端控件。当客户端需要访问内部网络中的C/S应用时,它从SSL VPN服务器下载控件。该控件是一个服务监听程序,它用于将客户端的C/S数据包转换为HTTP协议支持的连接方法,并通知SSL VPN服务器它所采用的通信协议(TCP或UDP)及要访问的目的服务地址和端口。客户机上的控件与SSL VPN服务器建立安全通道后,在本机上接收客户端的数据,并通过SSL通道将数据转发给SSL VPN服务器。SSL VPN服务器解密数据包后直接转发给内部网络中的目的服务器。SSL VPN服务器在接收到内部网络中目的服务器的响应数据包后,再通过SSL通道发送给客户端控件。客户端控件解密SSL数据包后转发给客户端应用程序。

3. SSL VPN的应用特点

在VPN应用中,SSL VPN属于较新的一项技术。相对于传统的VPN(如IPSec VPN),SSL VPN既有其应用优势,也存在不足。SSL VPN的主要优势如下。

(1) 可以不安装单独的客户端软件。虽然SSL VPN支持三种不同的工作模式,但在实际应用中多使用Web浏览器模式。Web浏览器模式不需要在客户端安装单独的客户端软件,只要使用标准的Web浏览器即可。

(2) 支持大多数设备。SSL VPN不仅仅支持在计算机上使用,而且还支持使用标准Web浏览器的PDA等移动设备。

(3) 安全性较高。SSL VPN在Internet等公共网络中通过使用SSL协议提供了安全的数据通道,并提供了对用户身份的认证功能。认证方式除了传统的用户名/密码方式外,还可以是数字证书、RADIUS等多种方式。SSL VPN能对加密隧道进行细分,从而使用户在浏览Internet上公有资源的同时,还可以访问单位内部网络中的资源。

(4) 方便部署。SSL VPN服务器一般位于防火墙内部,为了使用SSL VPN业务,只需要在防火墙上开启HTTPS协议使用的TCP 443端口即可。

(5) 支持的应用服务较多。通过SSL VPN,客户端目前可以方便地访问单位内部网络中的WWW、FTP、电子邮件和Windows"网上邻居"等常用的资源。目前,一些公司推出的SSL VPN产品已经能够为用户提供在线视频、数据库等多种访问。而且随着技术的不断发展,SSL VPN将会支持更多的访问服务。

虽然SSL VPN技术具有很多优势,但在应用中存在的一些不足也逐渐反映了出来,主要表现如下。

(1) 占用系统资源较大。SSL协议由于使用公匙密码算法,所以运算强度要比IPSec VPN大,需要占用较大的系统资源。所以SSL VPN的性能会随着同时连接用户数的增加而下降。

(2) 支持的应用有限。目前,大多数SSL VPN都是基于标准的Web浏览器而工作的,能够直接访问的主要是Web资源,其他资源的访问需要经过可Web化应用处理,系统的配置和维护都比较困难。另外,SSL VPN客户端对Windows操作系统的支持较好,但对UNIX、Linux等操作系统的支持较差。

另外,SSL VPN的稳定性还需要提高,同时许多客户端防火墙软件和防病毒软件都会对SSL VPN产生影响。

9.6 实验操作1 基于 Windows Server 2003 的 PPTP VPN 的实现

下面以图9-24所示的应用为例，介绍基于PPTP的VPN实现方法。其中客户端可通过Modem拨号、ADSL或局域网接入Internet，单位VPN服务器运行Windows Server 2003操作系统，并且已经采用公共IP地址连接到了Internet上。

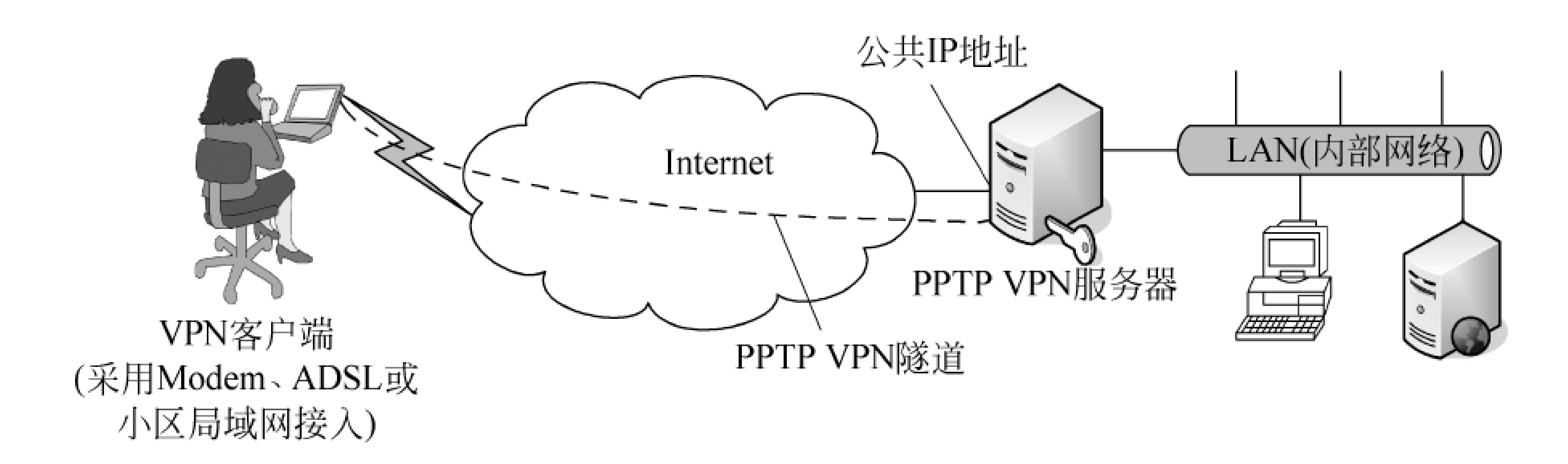


图9-24 基于PPTP VPN连接拓扑

9.6.1 安装和配置VPN服务器

由于不同单位网络接入和管理方式的不同，对于VPN服务器的网络连接和设置方式可能不同，但一般是在VPN服务器上安装两块网卡，其中一块网卡用于外网连接(设置在外网上使用的公共IP地址)，另一块网卡用于内部网络的连接(设置内部网络中使用的私有IP地址)。在此基础上，通过以下方法安装和配置PPTP VPN服务器。

(1) 选择"开始"→"程序"→"管理工具"→"路由和远程访问"，在打开的"路由和远程访问"窗口中选取服务器名称WLDHJ(本地)，单击鼠标右键，在弹出的快捷菜单中选择"配置并启用路由和远程访问"命令，如图9-25所示。

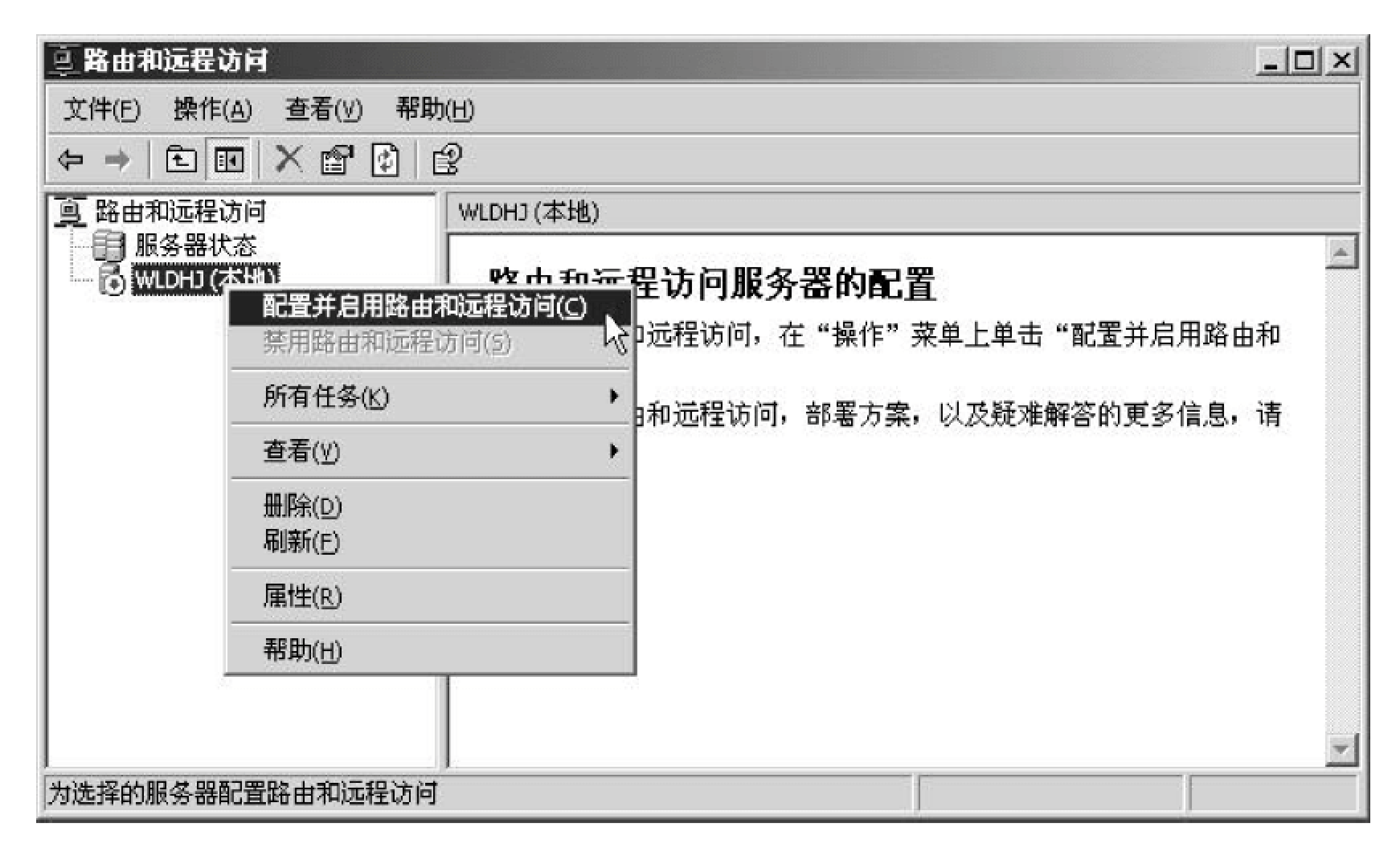


图9-25 配置并启用路由和远程访问

（2）在出现的“路由和远程访问服务器安装向导”对话框中，直接单击“下一步”按钮，在打开的如图 9-26 所示的对话框中选取“远程访问(拨号或 VPN)”单选按钮。

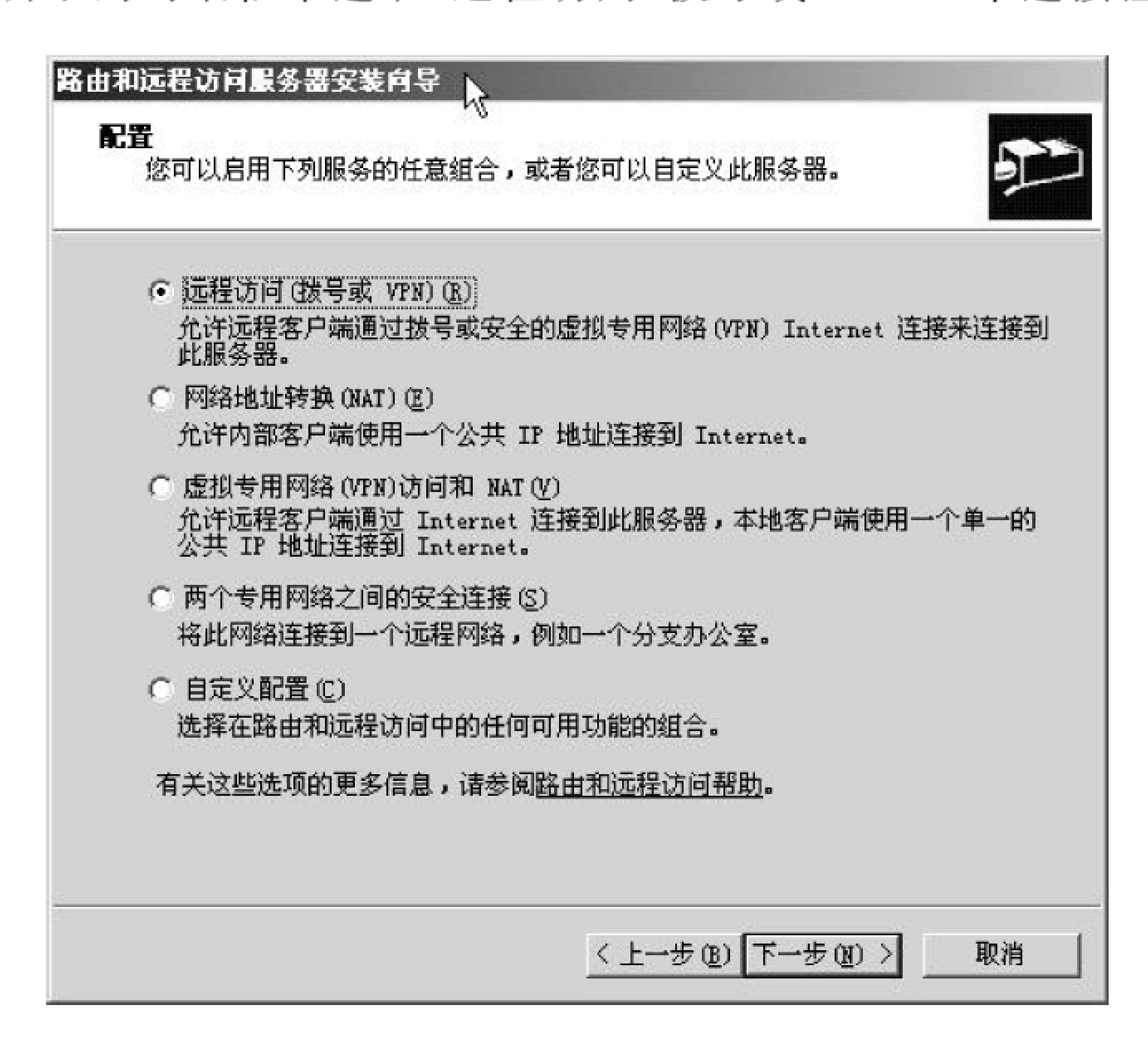


图 9-26　选取“远程访问(拨号或 VPN)”单选按钮

（3）单击“下一步”按钮，在出现的如图 9-27 所示的对话框中选取 VPN 复选框。

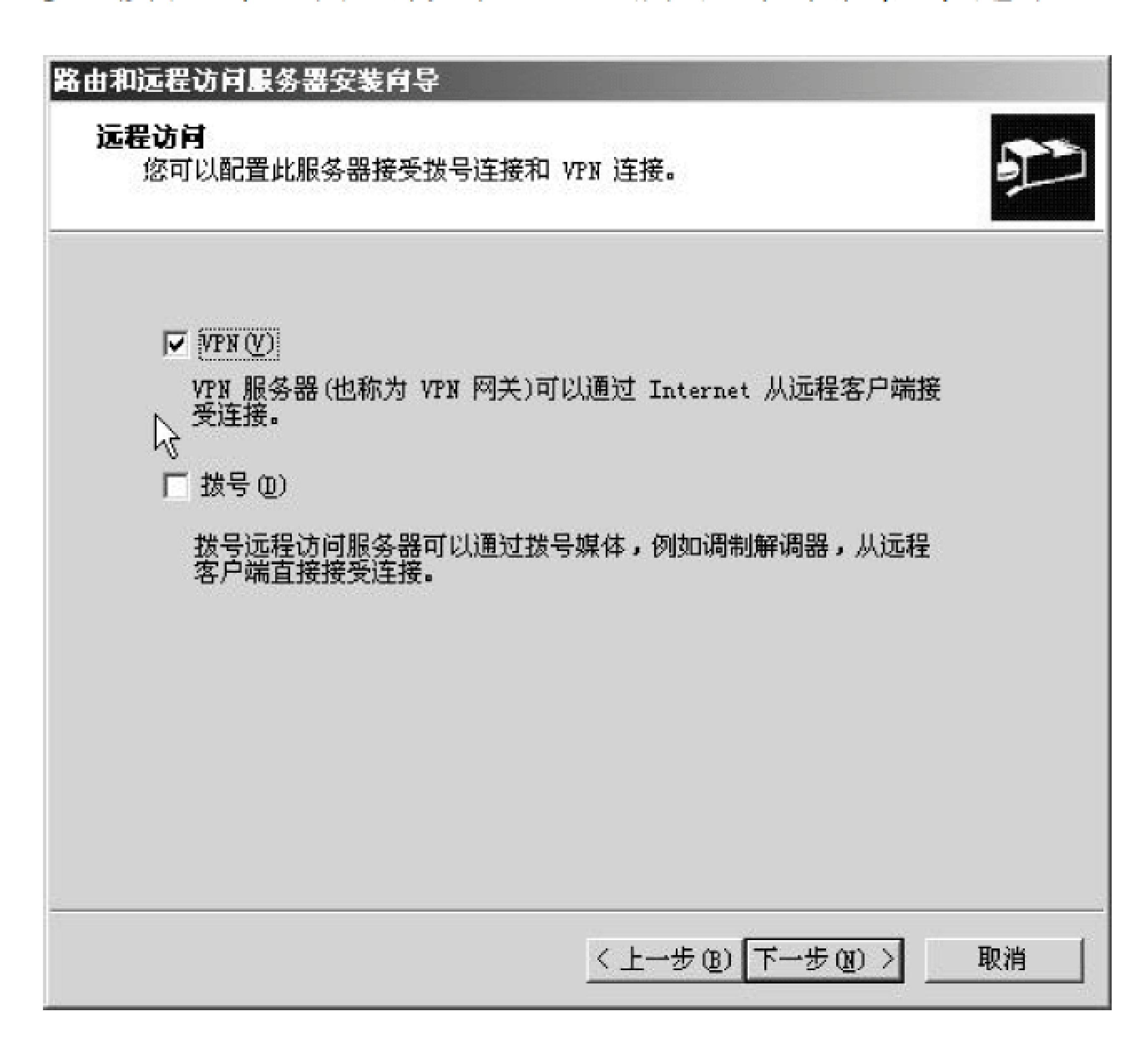


图 9-27　选取 VPN 远程访问方式

（4）单击“下一步”按钮，在打开的如图 9-28 所示的对话框中选择用来连接 Internet 的网卡(本地连接)，该网卡使用的是连接外部网络的公共 IP 地址。

其中，当选取“通过设置静态数据包筛选器来对选择的接口进行保护”复选框后，VPN 服务器会限制只有 VPN 的数据包才可以通过此网卡进入内部网络，其他的 IP 数据包到该 VPN 服务器时将被拒绝，从而增强 VPN 系统的安全性。不过，当选取了该复选框后，通过

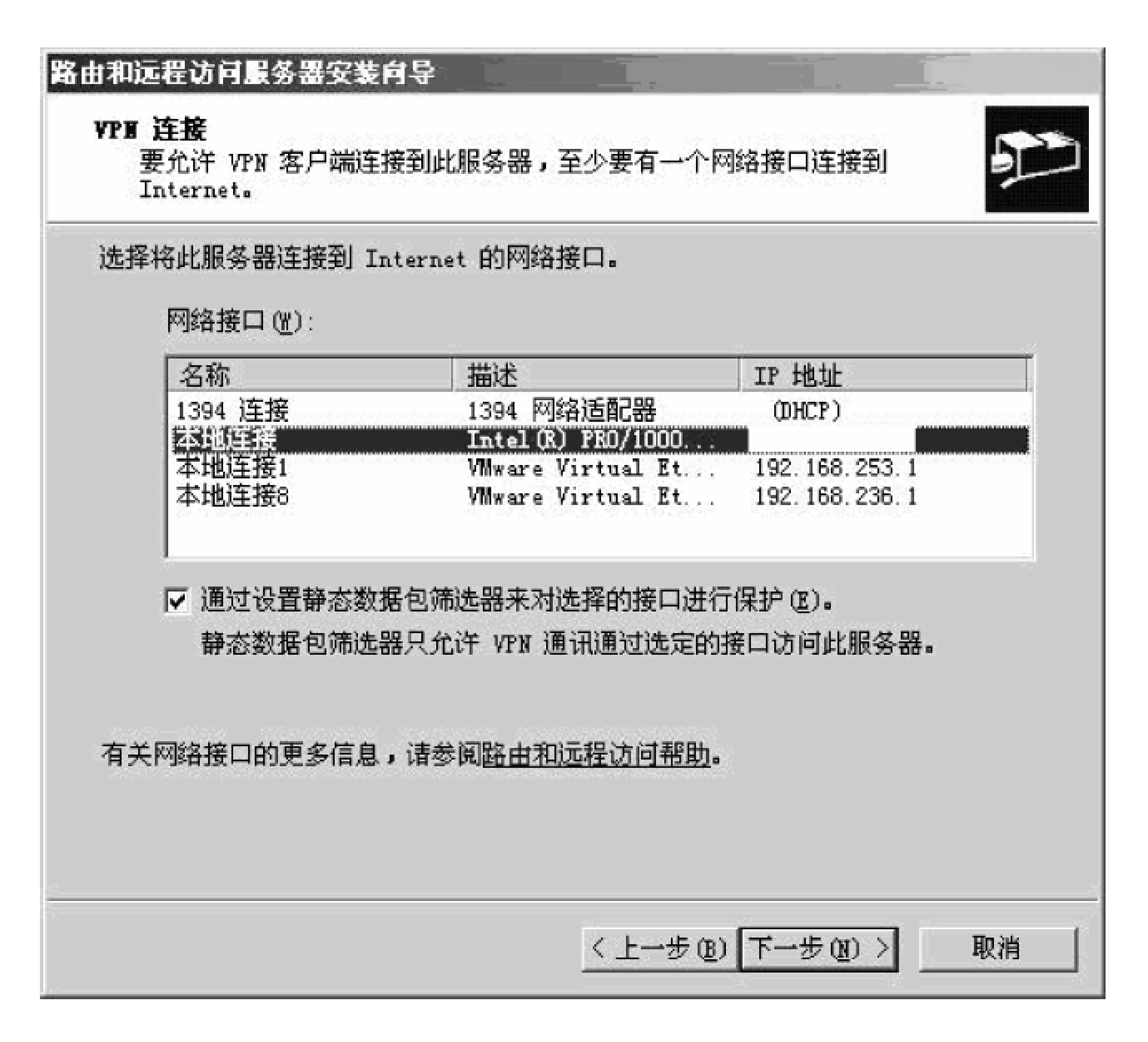


图 9-28　选择与 Internet 连接的网卡

该网站只能与 VPN 客户端进行通信，而无法与非 VPN 客户端进行通信。如果是专用的 VPN 服务器，建议选取此复选框。

(5) 单击"下一步"按钮，在出现的如图 9-29 所示的对话框中选取与内网连接的网卡(本地连接 1)。



图 9-29　选择与内网连接的网卡

(6) 单击"下一步"按钮，打开如图 9-30 所示的对话框。其中各选项的含义如下。

- 自动。由 VPN 服务器向网络中的 DHCP 服务器先租用 IP 地址，然后再分配给客户端使用。如果该网络中没有 DHCP 服务器，则该远程访问服务器将会自动向客户端分配 169.254.*.* 的 IP 地址(其中 * 代表的范围为 1～254)。

• 来自一个指定的地址范围。如果选择了此项，在单击“下一步”按钮后，则需要在打开的对话框中设置要分配给客户端的 IP 地址范围。

（7）在图 9-30 中选取“自动”单选按钮，单击“下一步”按钮，将打开如图 9-31 所示的对话框。在本例中选取“否，使用路由和远程访问来对连接请求进行身份验证”单选按钮。



图 9-30　选择 IP 地址指定方式

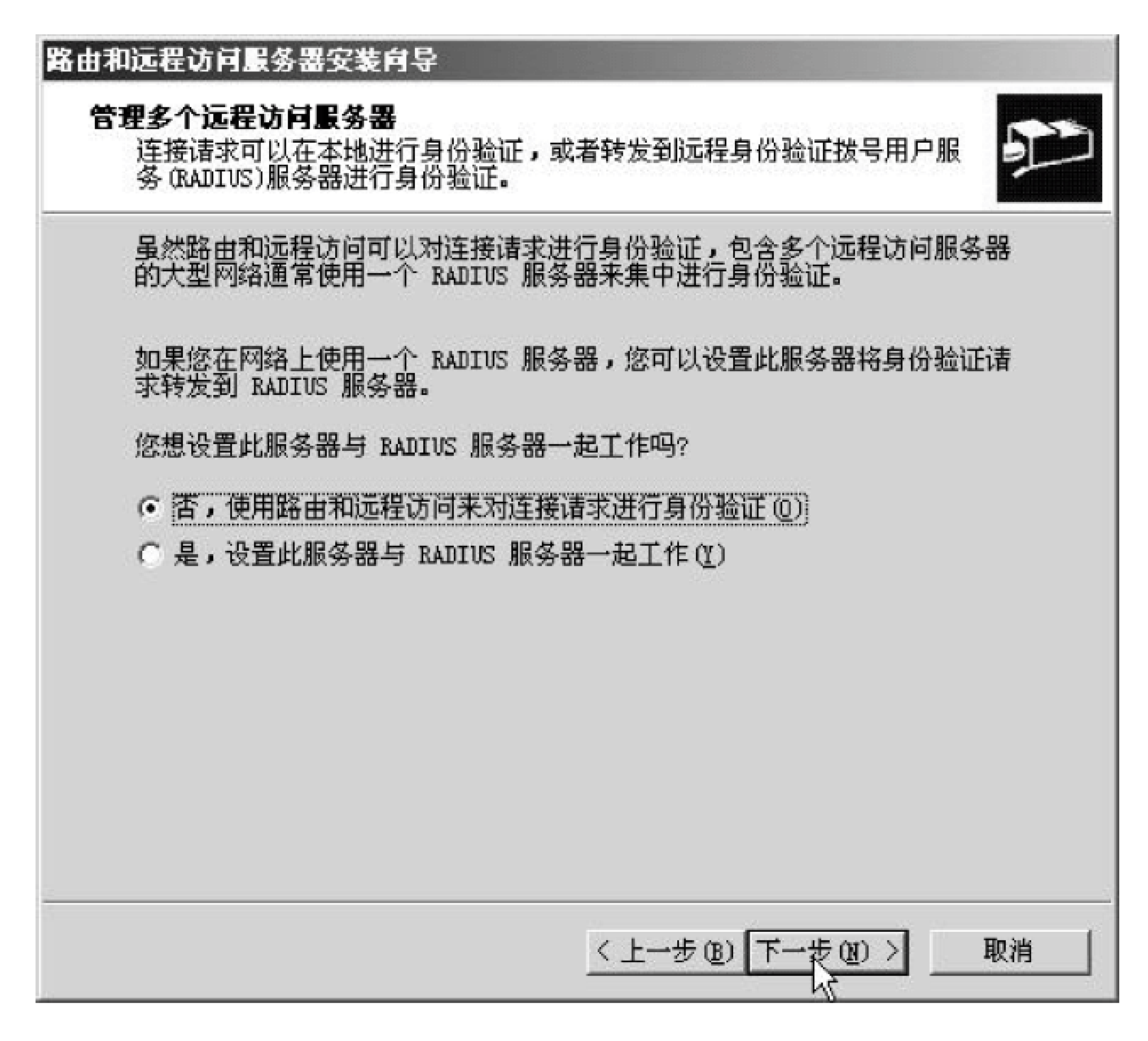


图 9-31　选择身份验证方式

单击“下一步”按钮，按系统默认方式完成配置。配置结束后，将显示如图 9-32 所示的窗口。系统默认会自动建立 128 个 PPTP 端口与 128 个 L2TP 端口，每一个端口可供一个 VPN 客户端建立连接使用。

在日常应用中，用于 VPN 连接的用户数一般是确定的。这样，管理人员可以根据实际

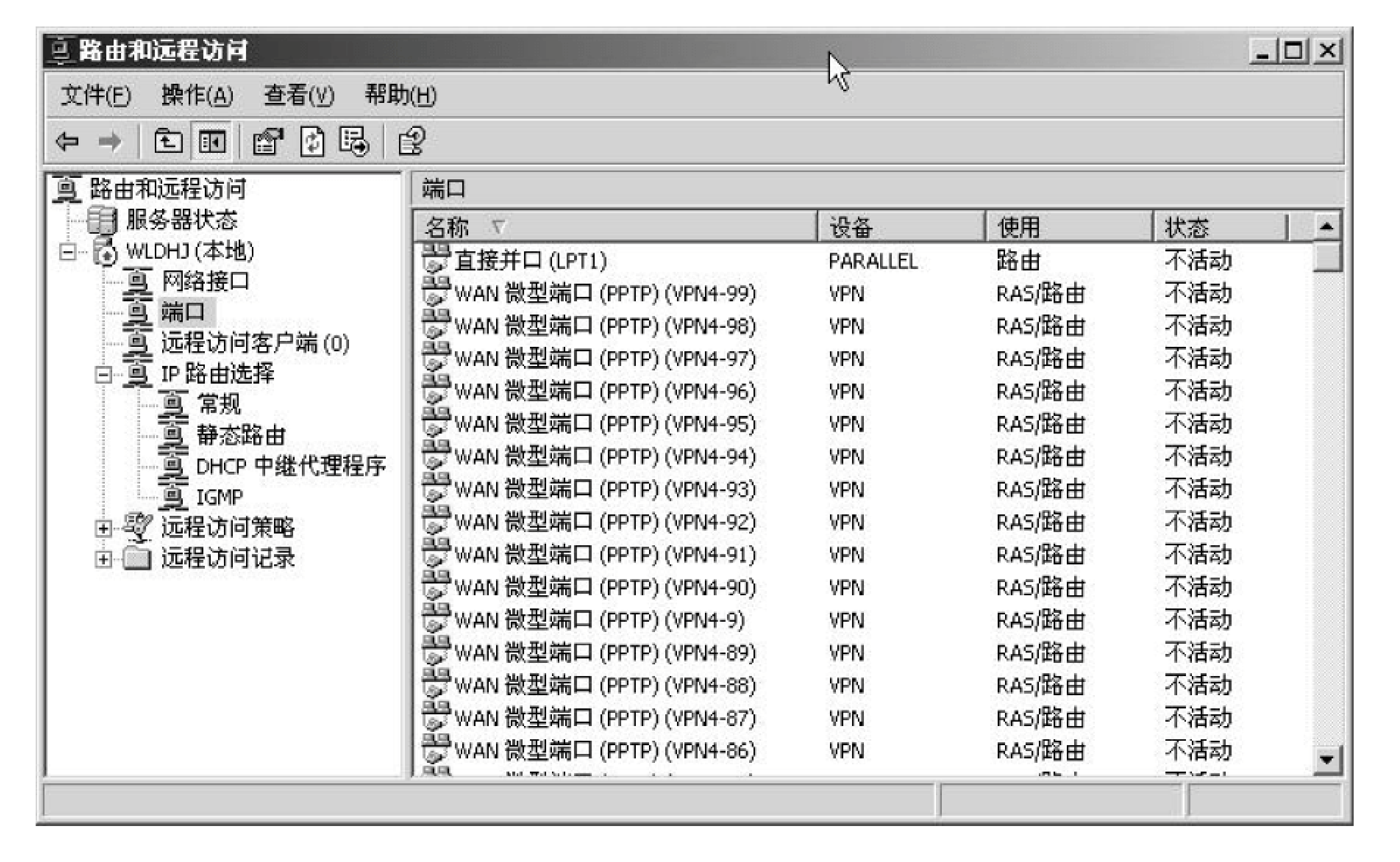


图 9-32　系统提供的 VPN 端口

分配的 VPN 用户数增加或减少 VPN 端口的数量。具体方法为：在如图 9-32 所示的窗口中选取“端口”，单击鼠标右键，在弹出的快捷菜单中选择“属性”命令，将打开如图 9-33 所示的“端口属性”对话框。选取使用的端口协议（本例为 PPTP），然后单击“配置”按钮，在打开的如图 9-34 所示的对话框中重新配置 VPN 端口的数量。

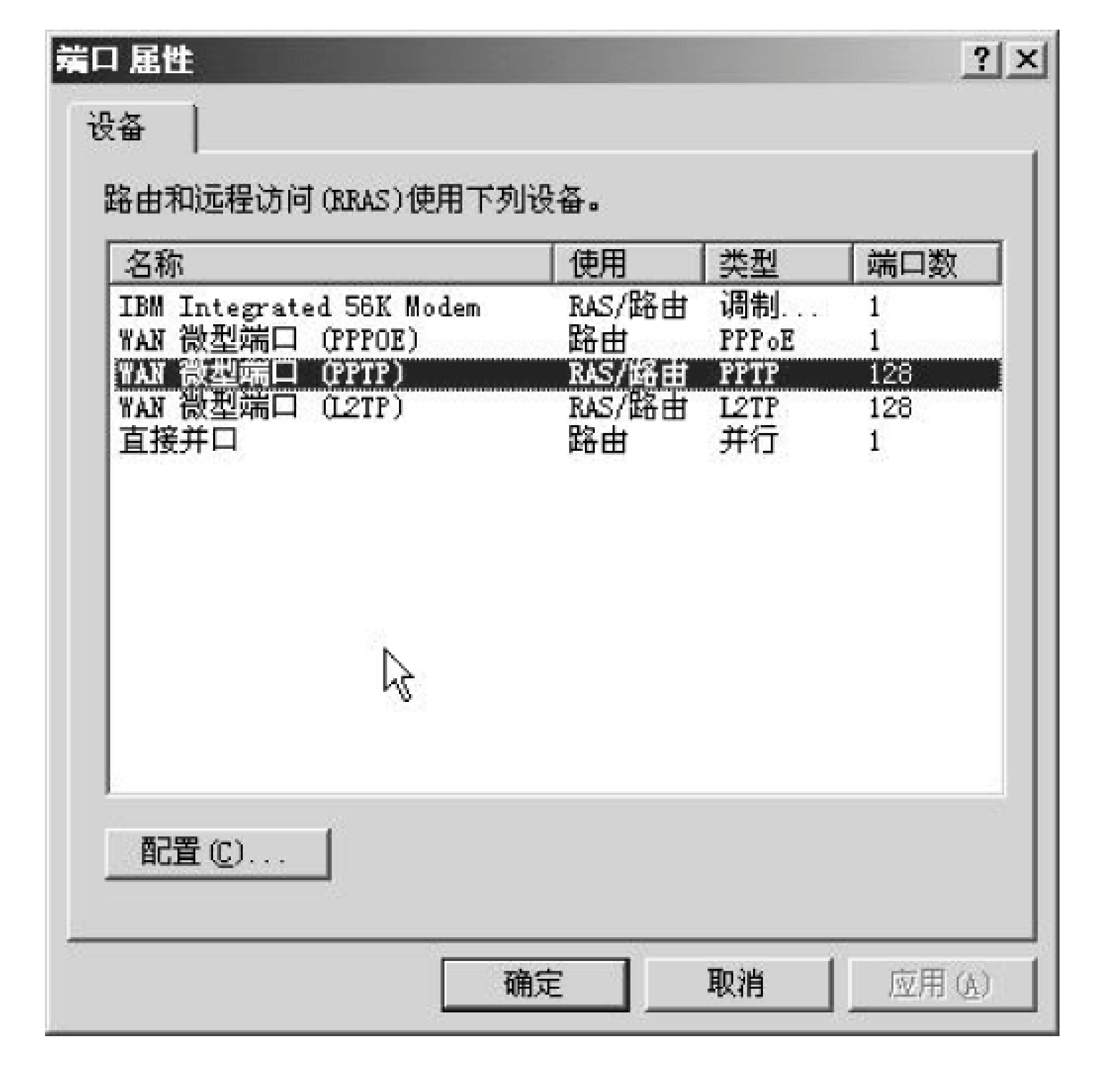


图 9-33　选择 PPTP 对应的端口

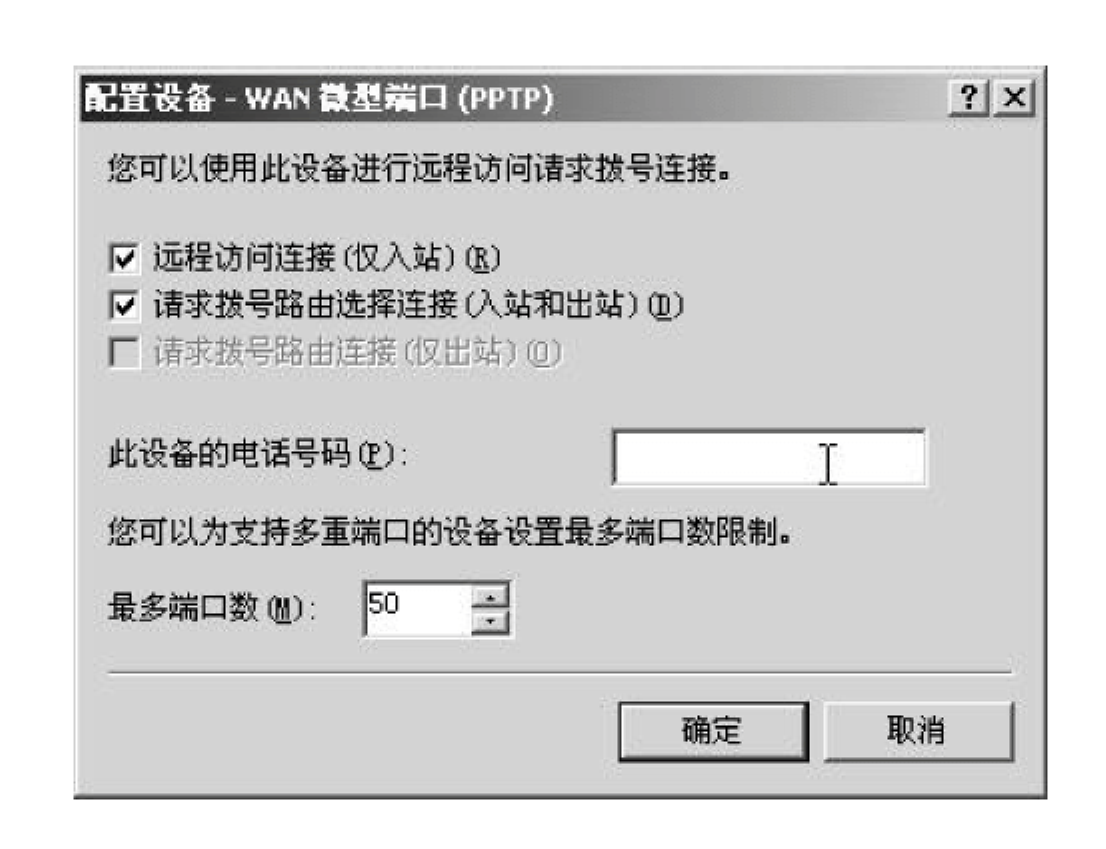


图 9-34　重新设置最多端口数

9.6.2　为用户分配远程访问权限

系统默认所有用户都不具有远程访问的权限，这时 VPN 客户端是无法连接到该 VPN 服务器的。可以通过以下方法来添加远程 VPN 用户。由于 VPN 服务器不一定是一台域控制器，所以下面的设置也要分两种情况。

1. VPN 服务器不是域控制器

当 VPN 服务器是一台运行 Windows Server 2003 的独立计算机时，可以通过以下的方法进行设置。

(1) 选择“开始”→“程序”→“管理工具”→“计算机管理”→“系统工具”→“本地用户和组”→“用户”，打开如图 9-35 所示的窗口。

(2) 在“用户”列表中选取要进行 VPN 拨号连接的用户账号(如 wq，这些账号需要事先创建)。单击鼠标右键，在弹出的快捷菜单中选择“属性”命令，在打开的对话框中选择“拨入”选项卡，打开如图 9-36 所示的对话框。首先在“远程访问权限(拨入或 VPN)”选项区域中选择“允许访问”单选按钮，然后在“回拨选项”选项区域中选择是否进行回拨。出于安全考虑，对于重要的一些远程访问，可以选择“总是回拨到”单选按钮，然后在后面的文本框中输入回拨的电话号码。这样，即使有人知道了远程用户的账户名称和密码，由于回拨的电话号码是固定的，所以该连接是安全的。

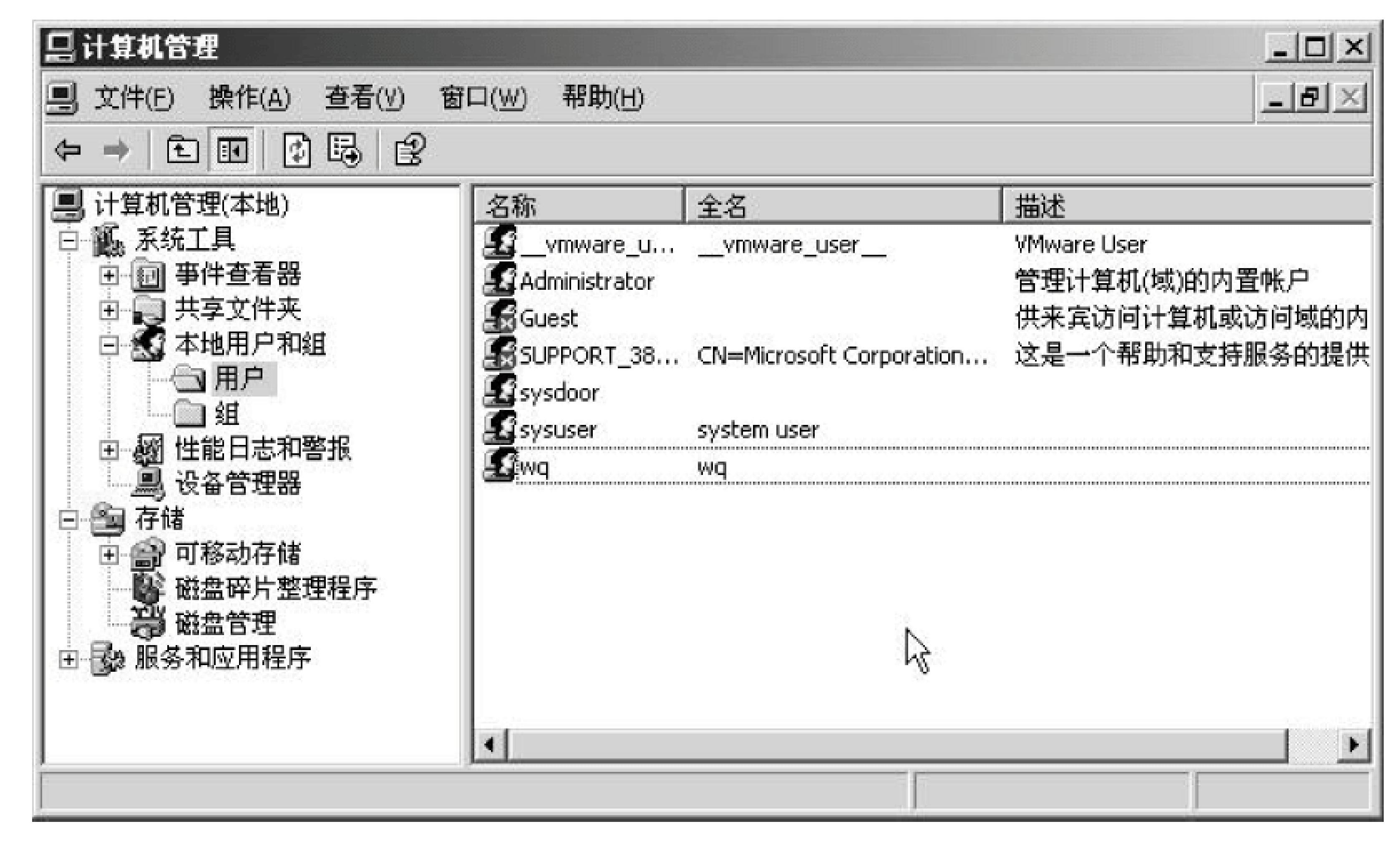


图 9-35 显示用户账号

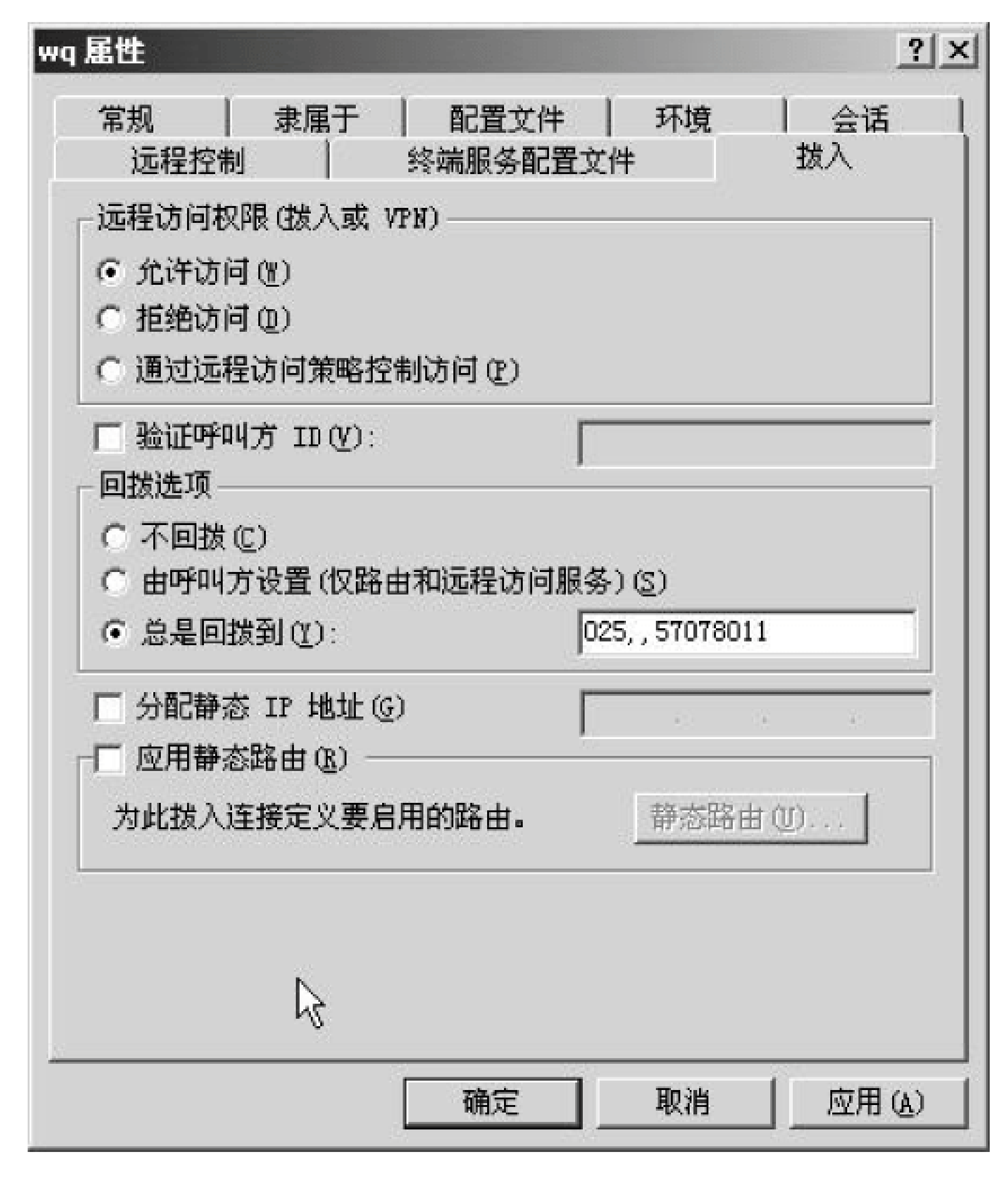


图 9-36 设置拨号属性

2. 远程访问服务器是域控制器

如果VPN服务器是一台运行活动目录(Active Directory)的域控制器,则可以通过以下的方法进行设置。

(1) 选择"开始"→"程序"→"管理工具"→"Active Directory 用户和计算机",打开"Active Directory 用户和计算机"窗口。

(2) 选取用户账号,单击鼠标右键,在弹出的快捷菜单中选择"属性"命令,在打开的对话框中选择"拨入"选项卡,将打开类似于如图9-36所示的对话框。设置方法与图9-36基本相同。

9.6.3 在VPN客户端建立VPN拨号连接

在确保VPN已经能够连接到Internet的前提下进行如下操作,本实验中所使用的操作系统为Windows XP Professional。关于客户端如何通过Modem拨号、ADSL拨号或局域网等方式接入Internet的方法读者可自行完成,在此不再赘述。

(1) 在桌面上选取"网上邻居",单击鼠标右键,在弹出的快捷菜单中选取"属性"命令,打开"网络连接"窗口。

(2) 单击"创建一个新的连接",出现"欢迎使用新建连接向导"对话框。

(3) 单击"下一步"按钮,在打开的如图9-37所示的对话框中选取"连接到我的工作场所的网络"单选按钮。

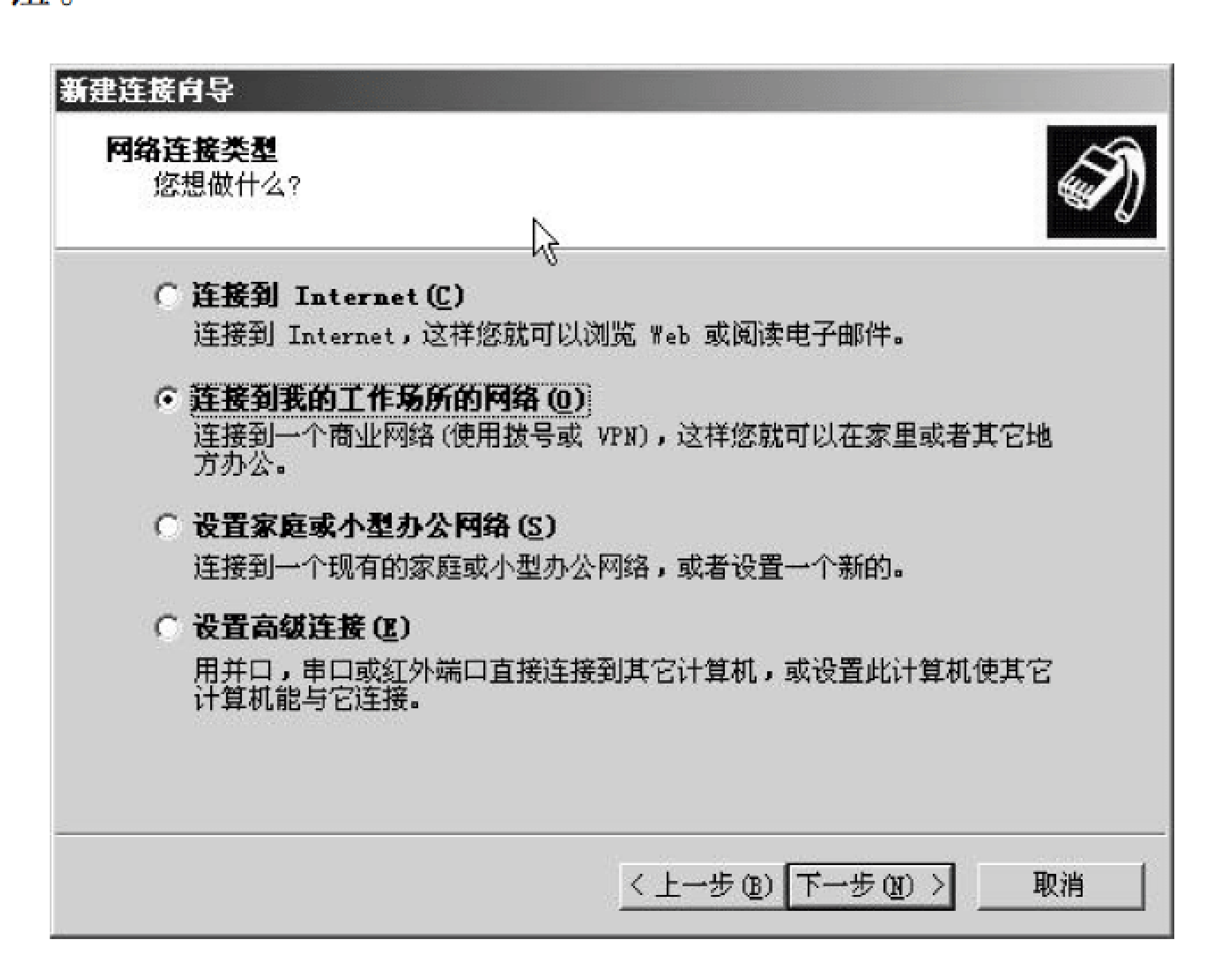


图9-37 选择网络连接类型

(4) 单击"下一步"按钮,在打开的如图9-38所示的对话框中选取"虚拟专用网络连接"单选按钮。

(5) 单击"下一步"按钮,在打开的如图9-39所示的对话框中的"公司名"文本框中输入VPN连接的名称。

(6) 单击"下一步"按钮,在打开的如图9-40所示的对话框中输入远程VPN服务器的IP地址。

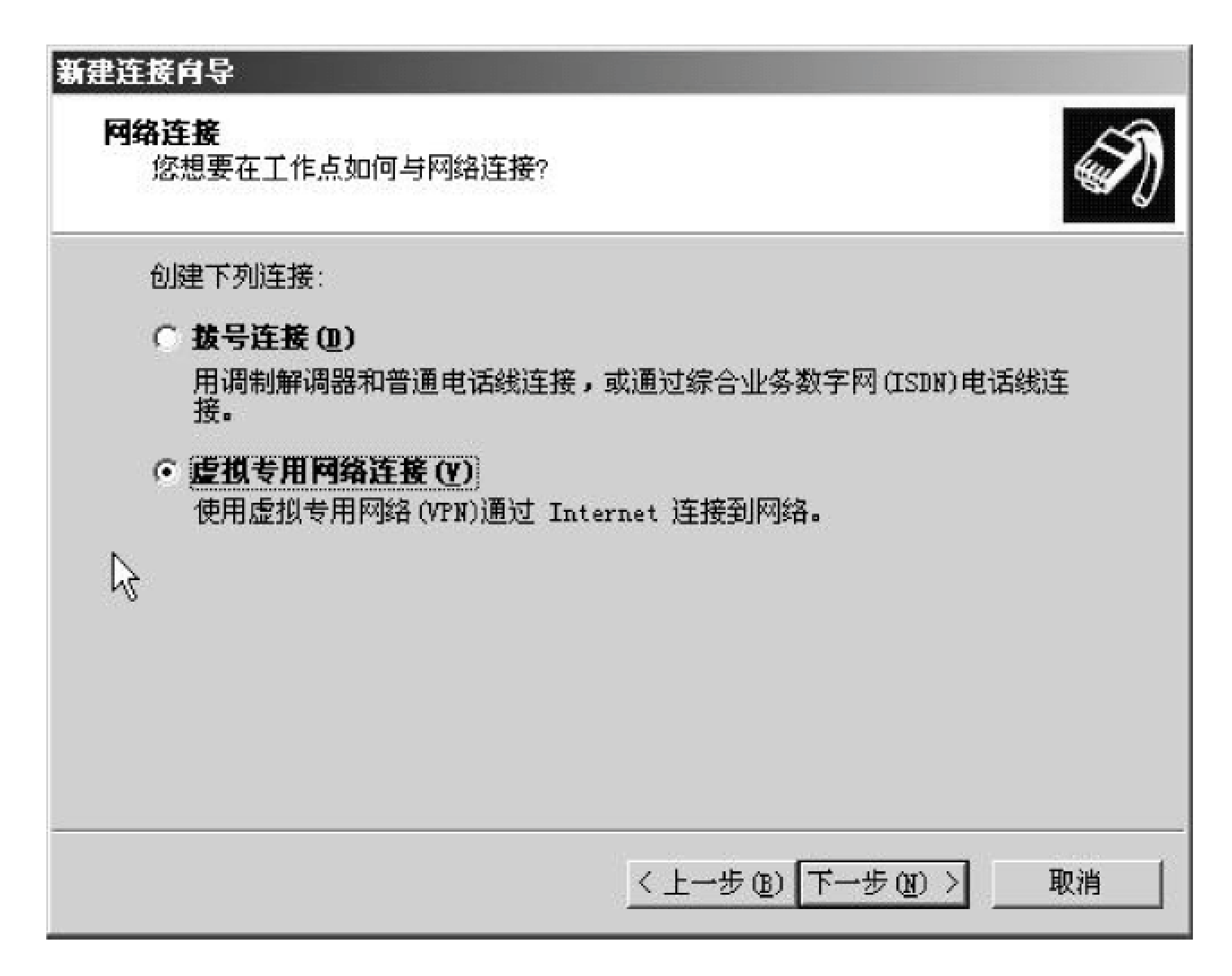


图 9-38 选取“虚拟专用网络连接”方式

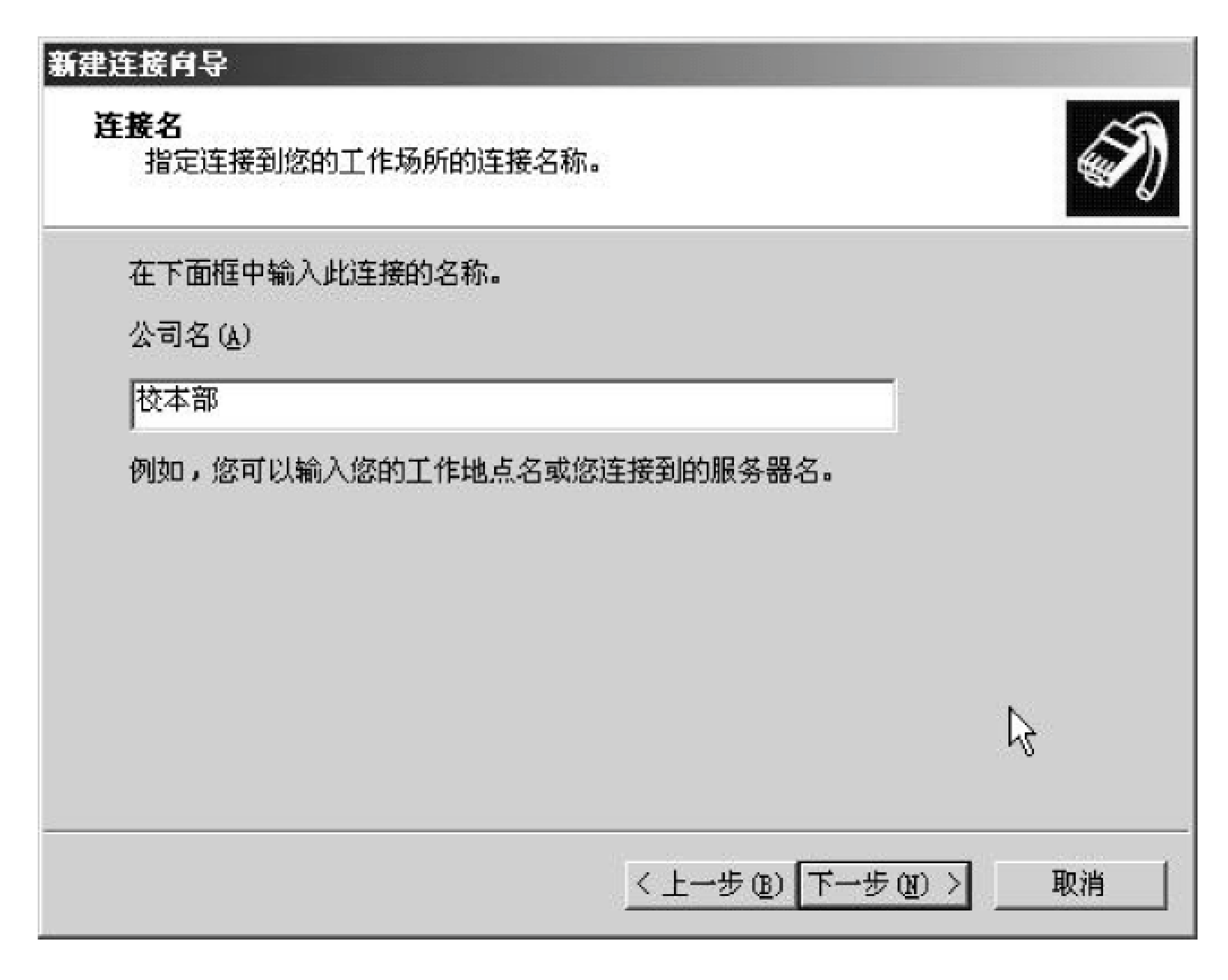


图 9-39 输入公司名称

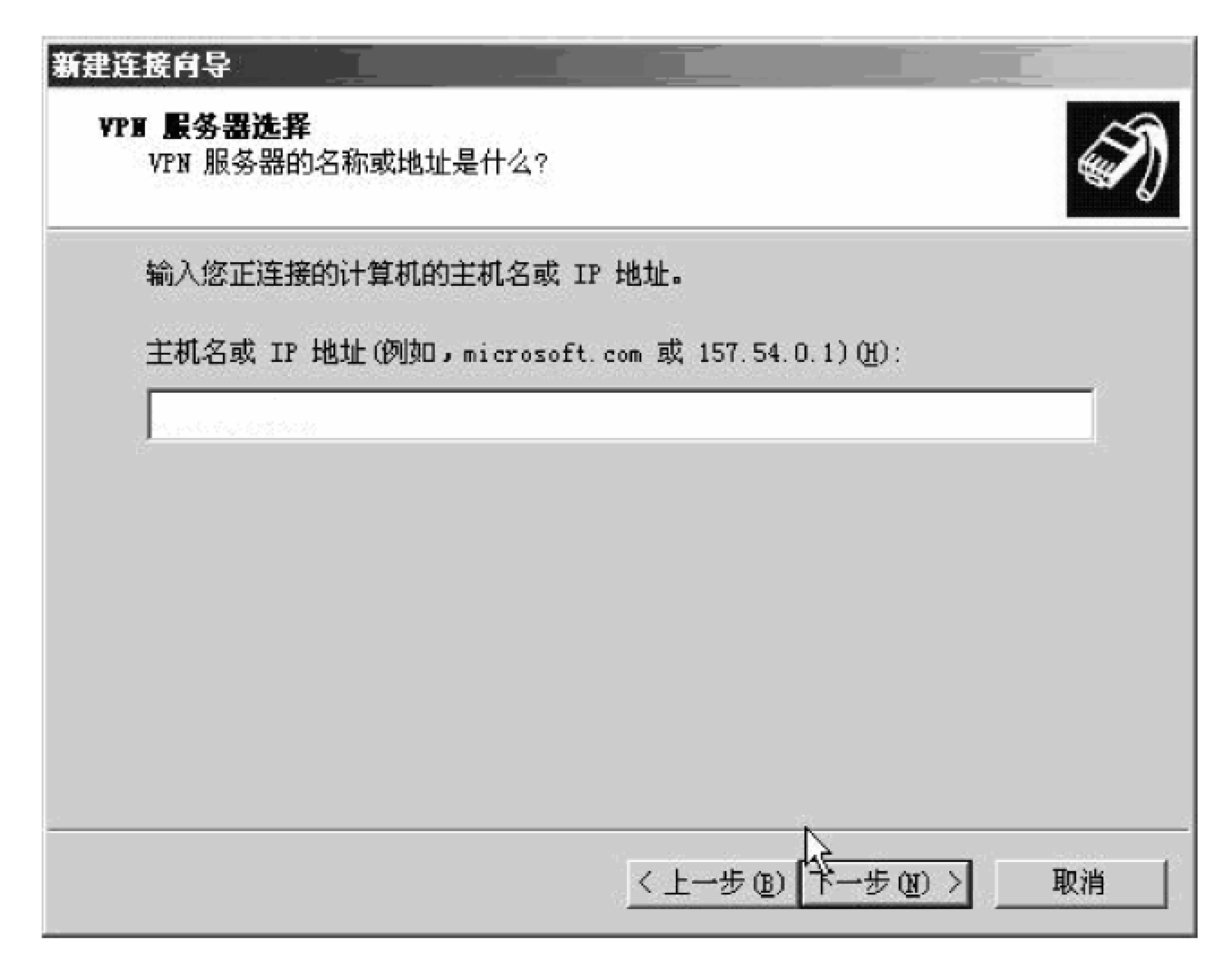


图 9-40 输入 VPN 服务器的 IP 地址

(7) 单击“下一步”按钮，打开如图 9-41 所示的对话框。当确认前面的设置无误后，单击“完成”按钮。为了便于将来的操作，建议选取“在我的桌面上添加一个到此连接的快捷方式”复选框。

之后，就可以通过已创建的 VPN 连接来登录 VPN 服务器，VPN 客户端的连接界面如图 9-42 所示。输入 VPN 用户的账号和对应的密码，就可以通过 PPTP 方式拨号到 VPN 服务器。

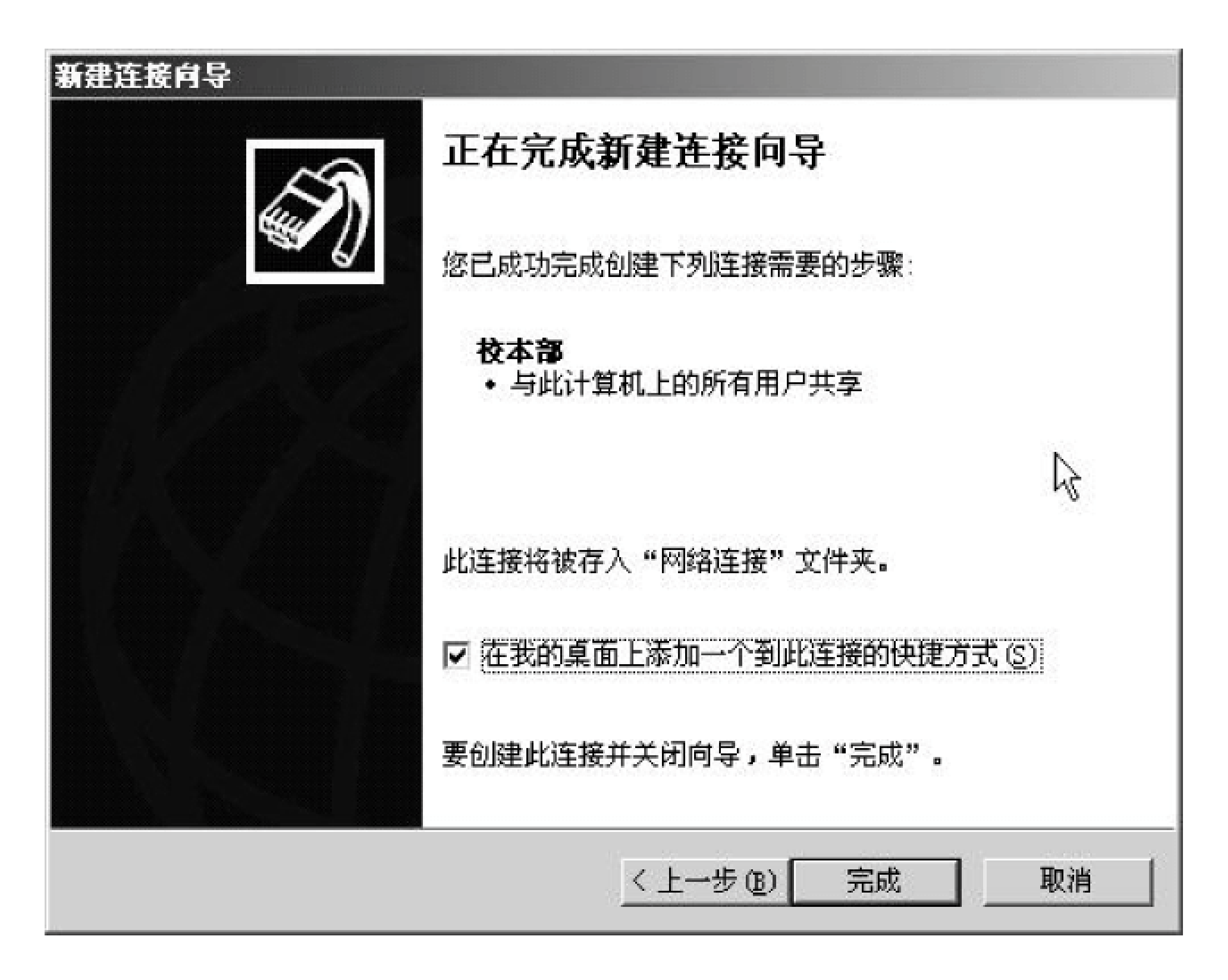


图 9-41　完成 VPN 客户端连接的建立



图 9-42　VPN 客户端拨号操作界面

需要注意的是，在进行 VPN 拨号连接之前，VPN 客户端必须先要能够连接到 Internet 上。

当 VPN 客户端连接到 VPN 服务器并成功建立了 VPN 连接后，就可以与 VPN 服务器及 VPN 服务器端的局域网进行通信。通信中既可以使用对方的 IP 地址(如图 9-43 所示)，也可以使用对方的计算机名称(NetBIOS 计算机名称，如图 9-44 所示)，使用方法与局域网内部没有什么区别。同时，也可以通过 Web 方式访问内部网络中的可 Web 化应用资源，如内部网络中的 Web 服务、FTP 服务、Webmail 服务等。

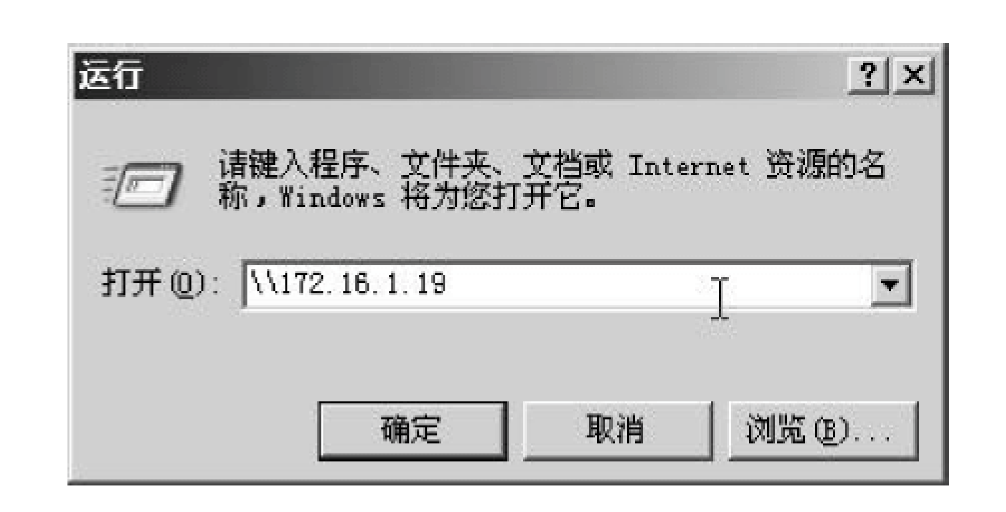


图 9-43　通过 IP 地址进行访问



图 9-44　通过对方计算机名称进行访问

管理员可以在 VPN 服务器上通过检查 VPN 端口的使用情况来查看目前有多少个 VPN 用户连接在该服务器上，如图 9-45 所示。其中，“状态”为“活动”的端口表示正在使用，“活动”端口的数量反映了 VPN 连接的用户数。

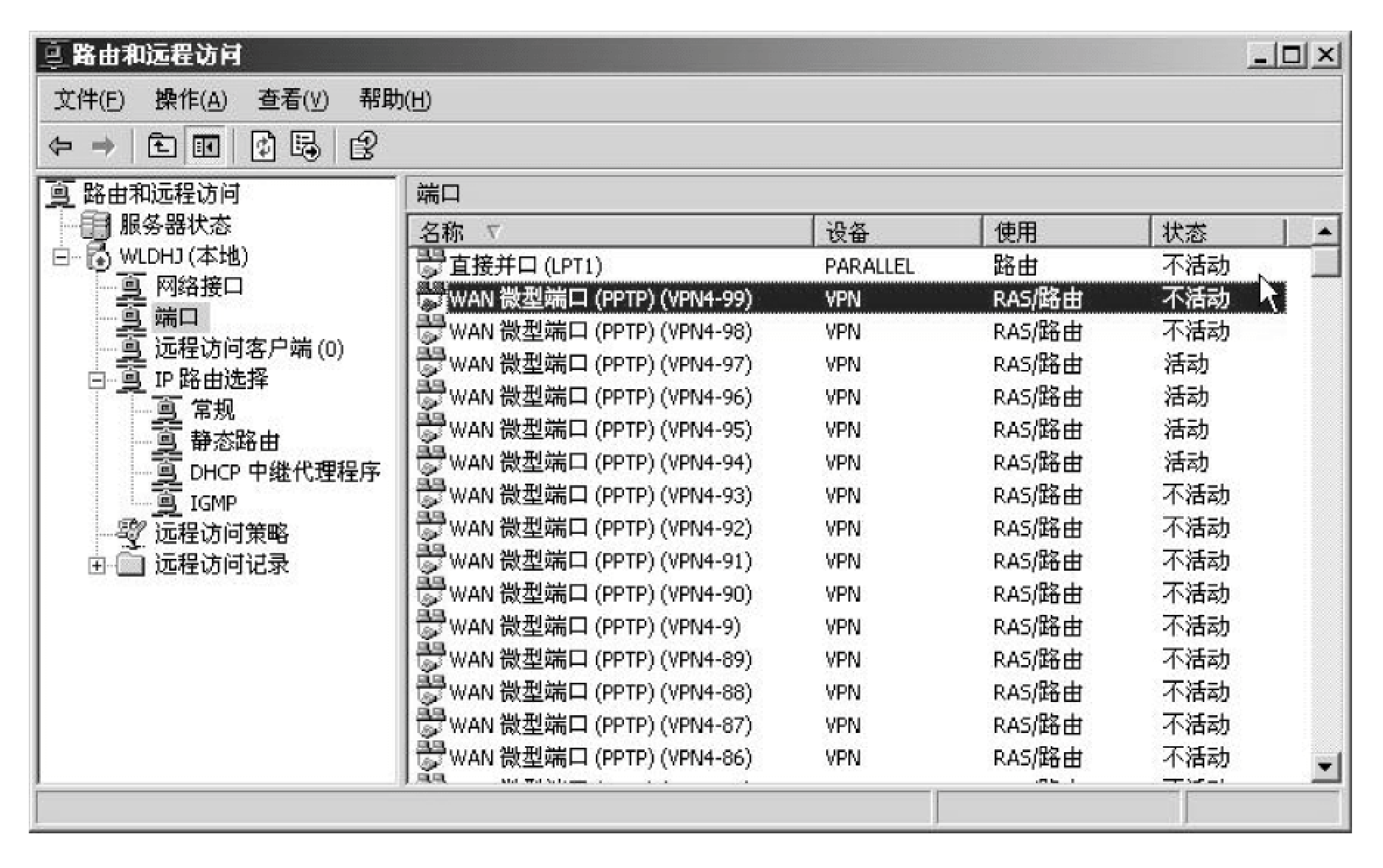


图 9-45　通过端口状态查看 VPN 的连接情况

习　　题

9-1　什么是 VPN 技术？与传统的应用专线连接相比，VPN 有何特点？

9-2　分别介绍内联网 VPN、外联网 VPN 和远程接入 VPN 的组网特点。

9-3　结合图 9-5 所示的隧道工作示意图，描述隧道的工作原理及应用特点。

9-4　在隧道建立过程中，主动式隧道与被动式隧道有何不同？

9-5　结合 OSI 参考模型各层的功能划分，试分析第二层隧道协议和第三层隧道协议的实现原理及应用特点。

9-6　对比分析第二层隧道协议 LLTP、L2TP 和 L2F 的实现原理及应用特点。

9-7　简述 GRE 隧道的形成过程及应用特点。

9-8　分析 IPSec 的安全体系，掌握 IKE、AH 和 ESP 的功能及实现方法。

9-9　结合 IP 技术和 ATM 技术，介绍 MPLS 的技术优势及实现原理。

9-10　结合 MPLS 的实现原理，介绍 MPLS VPN 的数据转发过程。

9-11　与 MPLS VPN 相比，SSL VPN 有何应用特点？

9-12　简述基于标准 Web 浏览器方式的 SSL VPN 的工作过程。

9-13　利用单位网络（如校园网）已有的条件，组建一台 VPN 服务器，供用户在外部（如家中）拨号来访问内部的网络资源。

参 考 文 献

1 张小琳. UTM 整合网络安全[J]. 北京：中国教育网络，2007(7)

2 肖海霞，等. 序列密码应用分析[J]. 江西：井冈山学院学报(自然科学)，2007(6)

3 吴行军，等. TEA 密码算法的 VLSI 实现[J]. 北京：半导体学报，2001(8)

4 方淡玉. ECC 公钥密码体制发展的未来[J]. 成都：信息安全与通信保密，2005(6)

5 肖皇培，等. 基于 Hash 函数的报文鉴别方法[J]. 上海：计算机工程，2007(3)

6 安晓龙，等. PKI 体系架构设计策略分析[J]. 北京：当代通信，2004(6)

7 蒋辉柏，等. PKI 中几种信任模型的分析研究[J]. 北京：计算机测量与控制，2003(11)

8 刘火斤，等. CRL 与 OCSP 相结合的证书撤销方案[J]. 北京：通信技术，2003(12)

9 王福，等. 基于 OCSP 方式的证书撤销策略[J]. 北京：计算机工程，2007(8)

10 胡廉民. 基于分层信任模型的 PKI 机构证书更新研究[J]. 北京：通信技术，2007(8)

11 张基温，等. 基于 PMI 的安全匿名授权体系[J]. 北京：计算机工程与设计，2007(2)

12 谭强，等. PMI 原理及实现初探[J]. 北京：计算机工程，2002(8)

13 周小为. PKI、PMI 技术研究[J]. 北京：计算机安全，2007(2)

14 李明柱(北京邮电大学信息安全中心). PKI 技术及应用开发指南[J]. http://www.ibm.com/developerworks/cn/security/se-pkiusing/index.html

15 李传目. 安全密码认证机制的研究[J]. 北京：计算机工程与应用，2003(8)

16 戚文静，等. 几种身份认证技术的比较及其发展方向[J]. 济南：山东建筑工程学院学报，2004(6)

17 赵洁，等. 基于虹膜的网络身份认证研究[J]. 北京：计算机应用研究，2005(7)

18 黄林，等. SSL 协议的分析和应用[J]. 合肥：电脑知识与技术，2007(2)

19 常强林，等. RADIUS 服务器的实现及其在宽带网计费系统中的应用[J]. 南京：军事通信技术，2003(2)

20 方蕾，等. DNS 安全漏洞以及防范策略研究[J]. 西安：微电子学与计算机，2003(10)

21 董建平. 域名系统安全扩展(DNSSEC)[J]. 北京：数据通信，2005(6)

22 周开宇，等. PC 的守护神——个人防火墙[J]. 上海：信息网络安全，2001(5)

23 孔祥华. 个人防火墙技术的研究与探讨[J]. 北京：中国科技信息，2005(11)

24 陈幼雷，等. 个人防火墙技术的研究与探讨[J]. 北京：计算机工程与应用，2002(8)

25 http://www.rising.com.cn/

26 郝辉，等. VPN 及其隧道技术研究[J]. 北京：微电子学与计算机，2004(11)

27 杨威，等. 基于 IKE 的 IPSec 参数协商过程的研究[J]. 北京：计算机工程，2003(3)

28 包丽红，等. 基于 SSL 的 VPN 技术研究[J]. 北京：网络安全技术与应用，2004(5)

29 郭世泽，等. 揭开黑客的面纱[M]. 北京：人民邮电出版社，2003(7)

30 郭世泽，等. 网络安全——取证与蜜罐[M]. 北京：人民邮电出版社，2003(7)

31 高海英，等. VPN 技术[M]. 北京：机械工业出版社，2004(4)

32 [美]Mark Stamp 著. Information Security Principles and Practice(信息安全原理与实践)[M]. 杜瑞颖，等译. 北京：电子工业出版社，2007(5)

33 http://www.ietf.org

34 http://www.ieee.org/portal/site/iportals/

相关课程教材推荐

ISBN	书　　名	定价(元)
9787302120193	计算机网络教程	32.00
9787302153511	计算机网络实验教程	26.00
9787302161585	计算机网络协议教程(第二版)	38.00
9787302155218	计算机网络实用教程(第二版)	34.00
9787302150046	计算机网络设计教程(第二版)	29.00
9787302128649	数据通信与网络应用	33.00
9787302128793	信息对抗与网络安全	21.00
9787302143338	计算机网络技术及应用教程	28.00
9787302134848	网络技术应用教程	19.00
9787302172666	计算机广域网络教程(第二版)	
9787302175063	信息网络技术实践教程	

以上教材样书可以免费赠送给授课教师,如果需要,请发电子邮件与我们联系。

教学资源支持

敬爱的教师:

感谢您一直以来对清华版计算机教材的支持和爱护。为了配合本课程的教学需要,本教材配有配套的电子教案(素材),有需求的教师可以与我们联系,我们将向使用本教材进行教学的教师免费赠送电子教案(素材),希望有助于教学活动的开展。

相关信息请拨打电话 010-62776969 或发送电子邮件至 weijj@tup.tsinghua.edu.cn 咨询,也可以到清华大学出版社主页(http://www.tup.com.cn 或 http://www.tup.tsinghua.edu.cn)上查询和下载。

如果您在使用本教材的过程中遇到了什么问题,或者有相关教材出版计划,也请您发邮件或来信告诉我们,以便我们更好为您服务。

地址:北京市海淀区双清路学研大厦 A 座 708　　计算机与信息分社魏江江　收
邮编:100084　　电子邮件:weijj@tup.tsinghua.edu.cn
电话:010-62770175-4604　　邮购电话:010-62786544

《计算机网络管理技术》目录

ISBN 978-7-302-17257-4
王 群 编著